(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2025-506391
(P2025-506391A)
(43)公表日　令和7年3月11日(2025.3.11)

(51)国際特許分類　FI
H04L 41/40 (2022.01)　H04L 41/40

審査請求　未請求　予備審査請求　未請求　（全96頁）

(21)出願番号　特願2024-545964(P2024-545964)
(86)(22)出願日　令和5年2月1日(2023.2.1)
(85)翻訳文提出日　令和6年9月12日(2024.9.12)
(86)国際出願番号　PCT/US2023/061713
(87)国際公開番号　WO2023/150522
(87)国際公開日　令和5年8月10日(2023.8.10)
(31)優先権主張番号　63/306,007
(32)優先日　令和4年2月2日(2022.2.2)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/306,918
(32)優先日　令和4年2月4日(2022.2.4)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/321,614
最終頁に続く

(71)出願人　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国 ９４０６５ カリフォルニア州 レッドウッド ショアーズ，メール ストップ ５オーピー７ オラクル パークウェイ ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　チェ，ジンス
アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション内
最終頁に続く

(54)【発明の名称】　異なるクラウド環境間の通信における改善されたエンドツーエンドの待ち時間のための改良されたネットワークリンクアーキテクチャ

(57)【要約】
第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークとの間にネットワークリンクを作成するための技術が説明される。第２のクラウド環境内の顧客のテナンシに関連付けられたユーザが、第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスできるようにするために、第１のクラウド環境内の第１の仮想ネットワークが作成される。このネットワークリンクは、第１のクラウド環境および第２のクラウド環境にデプロイされている１つまたは複数のリンク有効化仮想ネットワークに基づいて作成される。

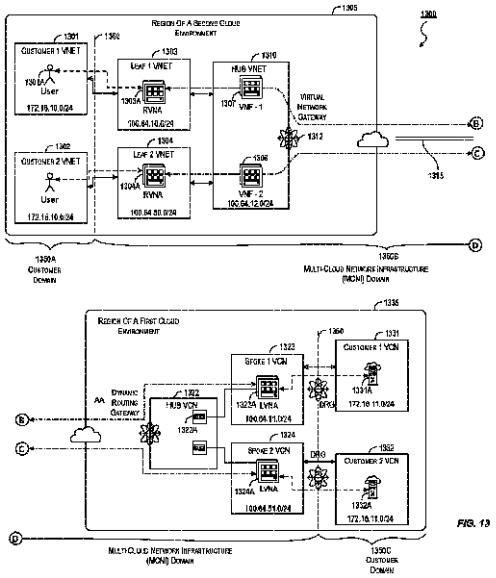

FIG. 13

【特許請求の範囲】
【請求項１】
方法であって、
第１のクラウド環境に含まれているマルチクラウドインフラストラクチャによって、前記第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークの間のネットワークリンクを作成する要求を受信することを含み、前記第２のクラウド環境内の顧客のテナンシに関連付けられたユーザが、前記第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスできるようにするために、前記第１のクラウド環境内の前記第１の仮想ネットワークは前もって作成されており、
前記方法は、複数のリンク有効化仮想ネットワークを使用して前記第１のクラウド環境内の前記第１の仮想ネットワークと前記第２のクラウド環境内の前記第２の仮想ネットワークの間に前記ネットワークリンクを作成することをさらに含み、前記複数のリンク有効化仮想ネットワークからの第１のリンク有効化仮想ネットワークは前記第２のクラウド環境に配置され、前記複数のリンク有効化仮想ネットワークからの第２のリンク有効化仮想ネットワークは前記第１のクラウド環境に配置される、方法。
【請求項２】
前記第２のクラウド環境内の前記第１のリンク有効化仮想ネットワークおよび前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークの各々に、固有のクラスレスドメイン間ルーティングＩＰアドレス空間が割り当てられる、請求項１に記載の方法。
【請求項３】
前記第２のクラウド環境内の前記第１のリンク有効化仮想ネットワークおよび前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークは、前記第２のクラウド環境の複数の顧客のテナンシの顧客のテナンシごとに作成される、請求項１に記載の方法。
【請求項４】
前記第１のリンク有効化仮想ネットワークは、前記第２のクラウド環境内の前記第２の仮想ネットワークから受信されたトラフィックをカプセル化して、カプセル化されたトラフィックを生成し、前記カプセル化されたトラフィックは、前記第１のリンク有効化仮想ネットワークによって前記第２のクラウド環境に含まれているハブ仮想ネットワークに送信される、請求項１に記載の方法。
【請求項５】
前記第１のリンク有効化仮想ネットワークは、仮想ネットワークアダプタの第１の対を含み、前記仮想ネットワークアダプタの各々は、前記第２のクラウド環境内の前記第２の仮想ネットワークから受信されたトラフィックをカプセル化して、カプセル化されたトラフィックを生成するように構成される、請求項１に記載の方法。
【請求項６】
前記第２のクラウド環境に含まれている前記ハブ仮想ネットワークは、仮想ネットワークフォワーダの対を含み、前記仮想ネットワークフォワーダの各々は、前記第１のリンク有効化仮想ネットワークから受信された、前記カプセル化されたトラフィックに対してネットワークアドレス変換を実行し、前記カプセル化されたトラフィックを前記第１のクラウド環境に含まれているハブ仮想ネットワークに転送するように構成される、請求項４に記載の方法。
【請求項７】
前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークは、仮想ネットワークアダプタの第２の対を含み、前記仮想ネットワークアダプタの各々は、前記第２のクラウド環境に含まれているハブ仮想ネットワークから受信された、カプセル化されたトラフィックをカプセル解除するように構成される、請求項１に記載の方法。
【請求項８】
前記第２のクラウド環境に含まれているハブ仮想ネットワークは、高帯域幅相互接続リンクによって、前記第１のクラウド環境に含まれているハブ仮想ネットワークに通信可能に結合される、請求項１に記載の方法。

【請求項９】
前記第１のクラウド環境に含まれている前記ハブ仮想ネットワークは、前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークに通信可能に結合されているＶＮＩＣを含む、請求項８に記載の方法。
【請求項１０】
前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークは、ダイナミックルーティングゲートウェイを介して、トラフィックを前記第１のクラウド環境内の前記第１の仮想ネットワークに転送する、請求項１に記載の方法。
【請求項１１】
コンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体であって、前記コンピュータ実行可能命令は、１つまたは複数のプロセッサによって実行された場合に、
第１のクラウド環境に含まれているマルチクラウドインフラストラクチャによって、前記第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークの間のネットワークリンクを作成する要求を受信することを引き起こし、前記第２のクラウド環境内の顧客のテナンシに関連付けられたユーザが、前記第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスできるようにするために、前記第１のクラウド環境内の前記第１の仮想ネットワークは前もって作成されており、
複数のリンク有効化仮想ネットワークを使用して前記第１のクラウド環境内の前記第１の仮想ネットワークと前記第２のクラウド環境内の前記第２の仮想ネットワークの間に前記ネットワークリンクを作成することをさらに引き起こし、前記複数のリンク有効化仮想ネットワークからの第１のリンク有効化仮想ネットワークは前記第２のクラウド環境に配置され、前記複数のリンク有効化仮想ネットワークからの第２のリンク有効化仮想ネットワークは前記第１のクラウド環境に配置される、コンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。
【請求項１２】
前記第２のクラウド環境内の前記第１のリンク有効化仮想ネットワークおよび前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークの各々に、固有のクラスレスドメイン間ルーティングＩＰアドレス空間が割り当てられる、請求項１１に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。
【請求項１３】
前記第２のクラウド環境内の前記第１のリンク有効化仮想ネットワークおよび前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークは、前記第２のクラウド環境の複数の顧客のテナンシの顧客のテナンシごとに作成される、請求項１１に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。
【請求項１４】
前記第１のリンク有効化仮想ネットワークは、前記第２のクラウド環境内の前記第２の仮想ネットワークから受信されたトラフィックをカプセル化して、カプセル化されたトラフィックを生成し、前記カプセル化されたトラフィックは、前記第１のリンク有効化仮想ネットワークによって前記第２のクラウド環境に含まれているハブ仮想ネットワークに送信される、請求項１１に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。
【請求項１５】
前記第１のリンク有効化仮想ネットワークは、仮想ネットワークアダプタの第１の対を含み、前記仮想ネットワークアダプタの各々は、前記第２のクラウド環境内の前記第２の仮想ネットワークから受信されたトラフィックをカプセル化して、カプセル化されたトラフィックを生成するように構成される、請求項１１に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。
【請求項１６】
前記第２のクラウド環境に含まれている前記ハブ仮想ネットワークは、仮想ネットワー

クフォワーダの対を含み、前記仮想ネットワークフォワーダの各々は、前記第１のリンク有効化仮想ネットワークから受信された、前記カプセル化されたトラフィックに対してネットワークアドレス変換を実行し、前記カプセル化されたトラフィックを前記第１のクラウド環境に含まれているハブ仮想ネットワークに転送するように構成される、請求項１４に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。

【請求項１７】

前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークは、仮想ネットワークアダプタの第２の対を含み、前記仮想ネットワークアダプタの各々は、前記第２のクラウド環境に含まれているハブ仮想ネットワークから受信された、カプセル化されたトラフィックをカプセル解除するように構成される、請求項１１に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。

【請求項１８】

前記第２のクラウド環境に含まれているハブ仮想ネットワークは、高帯域幅相互接続リンクによって、前記第１のクラウド環境に含まれているハブ仮想ネットワークに通信可能に結合される、請求項１１に記載のコンピュータ実行可能命令を格納する１つまたは複数のコンピュータ可読非一時的媒体。

【請求項１９】

１つまたは複数のプロセッサと、

命令を含んでいるメモリとを備えているコンピューティングデバイスであって、前記命令は、前記１つまたは複数のプロセッサを使用して実行された場合に、前記コンピューティングデバイスに、少なくとも、

第１のクラウド環境に含まれているマルチクラウドインフラストラクチャによって、前記第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークの間のネットワークリンクを作成する要求を受信することを実行させ、前記第２のクラウド環境内の顧客のテナンシに関連付けられたユーザが、前記第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスできるようにするために、前記第１のクラウド環境内の前記第１の仮想ネットワークは前もって作成されており、

複数のリンク有効化仮想ネットワークを使用して前記第１のクラウド環境内の前記第１の仮想ネットワークと前記第２のクラウド環境内の前記第２の仮想ネットワークの間に前記ネットワークリンクを作成することをさらに実行させ、前記複数のリンク有効化仮想ネットワークからの第１のリンク有効化仮想ネットワークは前記第２のクラウド環境に配置され、前記複数のリンク有効化仮想ネットワークからの第２のリンク有効化仮想ネットワークは前記第１のクラウド環境に配置される、コンピューティングデバイス。

【請求項２０】

前記第２のクラウド環境内の前記第１のリンク有効化仮想ネットワークおよび前記第１のクラウド環境内の前記第２のリンク有効化仮想ネットワークの各々に、固有のクラスレスドメイン間ルーティングＩＰアドレス空間が割り当てられる、請求項１９に記載のコンピューティングデバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、以下の仮出願の各々の非仮出願であり、以下の仮出願の各々の利益を主張する。下に挙げられた仮出願の各々の内容全体は、あらゆる目的で、参照によって本明細書に組み込まれている。

（１）２０２２年２月２日に出願された米国特許仮出願第６３／３０６，００７号、

（２）２０２２年２月４日に出願された米国特許仮出願第６３／３０６，９１８号、

（３）２０２２年３月１８日に出願された米国特許仮出願第６３／３２１，６１４号、

（４）２０２２年４月２２日に出願された米国特許仮出願第６３／３３３，９６５号、

（５）２０２２年４月２９日に出願された米国特許仮出願第６３／３３６，８１１号、
（６）２０２２年５月６日に出願された米国特許仮出願第６３／３３９，２９７号、
（７）２０２２年５月２６日に出願された米国特許仮出願第６３／３４６，００４号、
（８）２０２２年７月１４日に出願された米国特許仮出願第６３／３８９，３０５号、
（９）２０２２年７月１４日に出願された米国特許仮出願第６３／３８９，１４５号、および
（１０）２０２２年１０月２０日に出願された米国特許仮出願第６３／３８０，３２６号。

【０００２】

分野

本開示は、クラウドアーキテクチャに関し、より詳細には、１つのクラウド環境のユーザが、他のクラウド環境によって提供されたサービスを使用できるように、２つのクラウド環境をリンクするための技術に関する。

【背景技術】

【０００３】

背景

ここ数年、クラウドサービスの採用における劇的な増加が見られており、この傾向は増す一方である。さまざまなクラウド環境が、異なるクラウドサービスプロバイダ（ＣＳＰ：cloud service providers）によって提供されており、各クラウド環境は、一連の１つまたは複数のクラウドサービスを提供する。クラウド環境によって提供される一連のクラウドサービスは、ＳａａＳ（Software-as-a-Service）サービス、ＩａａＳ（Infrastructure-as-a-Service）サービス、ＰａａＳ（Platform-as-a-Service）サービスなどを含むが、これらに限定されない、１つまたは複数の異なる種類のサービスを含んでよい。

【０００４】

さまざまなクラウド環境が現在利用可能であるが、各クラウド環境は、閉じたエコシステムを加入している顧客に提供する。その結果、クラウド環境の顧客は、そのクラウド環境によって提供されたサービスを使用することに制限される。ＣＳＰによって提供されたクラウド環境に加入している顧客が、そのクラウド環境を介して、異なるＣＳＰによって提供された異なるクラウド環境において提供されているサービスを使用するための簡単な方法はない。本明細書において説明された実施形態は、これらの問題および他の問題に対処する。本明細書において説明された実施形態は、これらの問題および他の問題に対処する。

【発明の概要】

【０００５】

概要

本開示は、一般に、改善されたクラウドアーキテクチャに関し、より詳細には、１つのクラウド環境のユーザが、別の異なるクラウド環境によって提供されたサービスを使用できるように、２つのクラウドをリンクするための技術に関する。本明細書では、方法、システム、１つまたは複数のプロセッサによって実行可能なプログラム、コード、または命令を格納する非一時的コンピュータ可読ストレージ媒体などを含む、さまざまな実施形態が説明される。一部の実施形態は、コンピュータプログラム／命令を含んでいるコンピュータプログラム製品を使用することによって実装されてよく、これらのコンピュータプログラム／命令は、プロセッサによって実行された場合に、プロセッサに、本開示において説明された方法のいずれかを実行させる。

【０００６】

本開示の実施形態は、特定のクラウドネットワーク（例えば、Oracleクラウドインフラストラクチャ（ＯＣＩ：Oracle Cloud Infrastructure））のサービスを他のクラウド上の（例えば、Microsoft Azure内の）ユーザに配信するための機能をプロビジョニングする、マルチクラウド制御プレーン（ＭＣＣＰ：multi-cloud control plane

）フレームワークを提供する。ＭＣＣＰフレームワークは、ユーザのネイティブなクラウド環境のユーザ体験にできるだけ近いユーザ体験を提供しながら、（他のクラウド環境の）ユーザがクラウド環境のサービス（例えば、ＰａａＳサービス）にアクセスすることを可能にする。ＭＣＣＰの重要な課題は、顧客が、外部クラウド内のサービスの完全なデータプレーン機能を体験できるようになることである。

【０００７】

本開示の１つの実施形態は、第１のクラウド環境に含まれているマルチクラウドインフラストラクチャによって、第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークの間のネットワークリンクを作成する要求を受信することであって、第２のクラウド環境内の顧客のテナンシに関連付けられたユーザが、第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスできるようにするために、第１のクラウド環境内の第１の仮想ネットワークが前もって作成されている、受信することと、複数のリンク有効化仮想ネットワークを使用して第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークの間にネットワークリンクを作成することであって、複数のリンク有効化仮想ネットワークからの第１のリンク有効化仮想ネットワークが第２のクラウド環境に配置され、複数のリンク有効化仮想ネットワークからの第２のリンク有効化仮想ネットワークが第１のクラウド環境に配置される、作成することとを含む方法を対象にする。

【０００８】

本開示の態様は、１つまたは複数のデータプロセッサと、命令を含んでいる非一時的コンピュータ可読ストレージ媒体とを備えているコンピューティングデバイスを提供し、これらの命令は、１つまたは複数のデータプロセッサ上で実行された場合に、コンピューティングデバイスに、本明細書において開示された１つまたは複数の方法の一部またはすべてを実行させる。

【０００９】

本開示の別の態様は、１つまたは複数のデータプロセッサに、本明細書において開示された１つまたは複数の方法の一部またはすべてを実行させるように構成された命令を含む、非一時的機械可読ストレージ媒体において有形に具現化された、コンピュータプログラム製品を提供する。

【００１０】

前述の内容は、他の特徴および実施形態と共に、以下の明細書、特許請求の範囲、および添付の図面を参照するときに、さらに明らかになるであろう。

【００１１】

本開示の特徴、実施形態、および利点は、添付の図面を参照して以下の詳細な説明が読まれるときに、よりよく理解される。

【図面の簡単な説明】

【００１２】

【図１】ある実施形態による、クラウドサービスプロバイダインフラストラクチャによってホストされる仮想クラウドネットワークまたはオーバーレイクラウドネットワークを示す分散環境の高レベルの図である。

【図２】ある実施形態による、ＣＳＰＩ内の物理ネットワークにおける物理コンポーネントの簡略化されたアーキテクチャ図を示す図である。

【図３】ある実施形態による、ホストマシンが複数のネットワーク仮想化デバイス（ＮＶＤ：network virtualization devices）に接続されるＣＳＰＩ内の例示的な配置を示す図である。

【図４】ある実施形態による、マルチテナンシ機能をサポートするためのＩ／Ｏ仮想化を実現するための、ホストマシンとＮＶＤの間の接続を示す図である。

【図５】ある実施形態による、ＣＳＰＩによって提供された物理ネットワークの簡略化されたブロック図を示す図である。

【図６】ある実施形態による、異なるクラウドサービスプロバイダ（ＣＳＰ）によって提

供された複数のクラウド環境を含んでいる分散環境の簡略化された高レベルの図であり、クラウド環境が、その特定のクラウド環境によって提供された１つまたは複数のクラウドサービスが他のクラウド環境の顧客によって使用されることを可能にする特殊なインフラストラクチャを提供する特定のクラウド環境を含む。
【図７】一部の実施形態による、マルチクラウド制御プレーン（ＭＣＣＰ）の例示的な高レベルのアーキテクチャを示す図である。
【図８Ａ】一部の実施形態による、異なるクラウド環境内の２つのユーザアカウントをリンクするための例示的なプロセスを示す図である。
【図８Ｂ】一部の実施形態による、異なるクラウド環境内の２つのユーザアカウントをリンクするための例示的なプロセスを示す図である。
【図９】一部の実施形態による、マルチクラウド制御プレーン（ＭＣＣＰ）のコンポーネントを示す例示的なシステム図を示す図である。
【図１０】ある実施形態による、ネットワークリンクコンポーネントの高レベルのブロック図を示す図である。
【図１１】ある実施形態による、ネットワークリンクの詳細なアーキテクチャを示す図である。
【図１２Ａ】ある実施形態による、図１１のネットワークリンクのアーキテクチャに関して観察された例示的な待ち時間値を示す図である。
【図１２Ｂ】ある実施形態による、図１１のネットワークリンクのアーキテクチャに関して観察された例示的な待ち時間値を示す図である。
【図１２Ｃ】ある実施形態による、ネットワークリンクを確立するプロセスを示す例示的なフローチャートを示す図である。
【図１３】ある実施形態による、ネットワークリンクの別の詳細なアーキテクチャを示す図である。
【図１４Ａ】ある実施形態による、図１３のネットワークリンクのアーキテクチャに関して観察された例示的な待ち時間値を示す図である。
【図１４Ｂ】ある実施形態による、ネットワークリンクを確立するプロセスを示す別の例示的なフローチャートを示す図である。
【図１５】ある実施形態による、マルチクラウドサービス制御プレーンのシステム図を示す図である。
【図１６Ａ】ある実施形態による、異なるクラウド環境とのマルチクラウドサービス制御プレーンの情報のやりとりを示すスイム図を示す図である。
【図１６Ｂ】ある実施形態による、マルチクラウドサービス制御プレーンによって実行されるプロセスを示す例示的なフローチャートを示す図である。
【図１７Ａ】ある実施形態による、異なるクラウド環境の可用性ドメイン内の計算インスタンスの例示的な配置戦略を示す図である。
【図１７Ｂ】ある実施形態による、計算インスタンスが配置される異なるクラウド環境の可用性ドメインを決定することにおいてマルチクラウドサービス制御プレーンによって実行されるプロセスを示す例示的なフローチャートを示す図である。
【図１８】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための１つのパターンを示すブロック図である。
【図１９】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための別のパターンを示すブロック図である。
【図２０】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための別のパターンを示すブロック図である。
【図２１】少なくとも１つの実施形態による、サービスシステムとしてクラウドインフラストラクチャを実装するための別のパターンを示すブロック図である。
【図２２】少なくとも１つの実施形態による、例示的なコンピュータシステムを示すブロック図である。
【発明を実施するための形態】

【００１３】
詳細な説明
以下の説明では、説明の目的で、ある実施形態を十分に理解できるように、特定の詳細が示されている。しかし、さまざまな実施形態が、それらの特定の詳細なしで実践されてよいということが明らかである。各図および説明は、限定となるよう意図されていない。「例示的」という単語は、本明細書では「例、事例、または実例としての役割を果たす」ことを意味するために使用される。「例示的」として本明細書に記載されたすべての実施形態または設計は、必ずしも他の実施形態または設計よりも好ましいか、または有利であると解釈されるべきではない。
【００１４】
本開示は、一般に、改善されたクラウドアーキテクチャに関し、より詳細には、１つのクラウド環境のユーザが、別の異なるクラウド環境によって提供されたサービスを使用できるように、２つのクラウドをリンクするための技術に関する。本明細書では、方法、システム、１つまたは複数のプロセッサによって実行可能なプログラム、コード、または命令を格納する非一時的コンピュータ可読ストレージ媒体などを含む、さまざまな実施形態が説明される。一部の実施形態は、コンピュータプログラム／命令を含んでいるコンピュータプログラム製品を使用することによって実装されてよく、これらのコンピュータプログラム／命令は、プロセッサによって実行された場合に、プロセッサに、本開示において説明された方法のいずれかを実行させる。
【００１５】
本開示の実施形態は、特定のクラウドネットワーク（例えば、Oracleクラウドインフラストラクチャ（ＯＣＩ））のサービスを他のクラウド上の（例えば、Microsoft Azure内の）ユーザに配信するための機能をプロビジョニングする、マルチクラウド制御プレーン（ＭＣＣＰ）フレームワークを提供する。ＭＣＣＰフレームワークは、ユーザのネイティブなクラウド環境のユーザ体験にできるだけ近いユーザ体験を提供しながら、（他のクラウド環境の）ユーザがクラウド環境のサービス（例えば、ＰａａＳサービス）にアクセスすることを可能にする。ＭＣＣＰの重要な課題は、顧客が、外部クラウド内のサービスの完全なデータプレーン機能を体験できるようになることである。
【００１６】
ＭＣＣＰは、第２のクラウドインフラストラクチャのユーザ（例えば、Azureユーザ）が、ユーザにとって透過的な方法で、第１のクラウドインフラストラクチャ（例えば、ＯＣＩ）によって提供されたリソース（例えば、データベースリソース）を利用できるようにする。特に、第１のクラウドインフラストラクチャによって提供されたサービスは、第２のクラウドインフラストラクチャにおける「ネイティブな」サービスのように見える。これによって、第２のクラウドインフラストラクチャの顧客が、第１のクラウドインフラストラクチャによって提供されたサービスにネイティブにアクセスできるようにする。図６～図１７Ｂを参照して下で説明されるように、ＭＣＣＰは、外部クラウドユーザ（例えば、第２のクラウドインフラストラクチャのユーザ）によって利用される第１のクラウドインフラストラクチャのリソースを公開する、第１のクラウドインフラストラクチャにおいて実行されるマイクロサービスの集合である。これらのマイクロサービスの各々は、第１のクラウドインフラストラクチャによって提供されたリソースとの通信を提供するプロキシとして機能する。
【００１７】
クラウドネットワークの例
クラウドサービスという用語は、通常、クラウドサービスプロバイダ（ＣＳＰ）によって、ＣＳＰによって提供されたシステムおよびインフラストラクチャ（クラウドインフラストラクチャ）を使用しているユーザまたは顧客による利用をオンデマンドで（例えば、サブスクリプションモデルによって）可能にされるサービスのことを指すために使用される。通常、ＣＳＰのインフラストラクチャを構成するサーバおよびシステムは、顧客自身のオンプレミスのサーバおよびシステムから分離している。したがって、顧客は、サービ

スのための別々のハードウェアリソースおよびソフトウェアリソースを購入することを必要とせずに、ＣＳＰによって提供されたクラウドサービスを利用することができる。クラウドサービスは、加入している顧客に、顧客が、サービスを提供するために使用されるインフラストラクチャの調達に投資することを必要としない、アプリケーションおよびコンピューティングリソースへの容易で拡張可能なアクセスを提供するように設計される。

【００１８】

さまざまな種類のクラウドサービスを提供する、複数のクラウドサービスプロバイダが存在する。ＳａａＳ（Software-as-a-Service）、ＰａａＳ（Platform-as-a-Service）、ＩａａＳ（Infrastructure-as-a-Service）などを含む、クラウドサービスのさまざまな種類またはモデルが存在する。

【００１９】

顧客は、ＣＳＰによって提供された１つまたは複数のクラウドサービスに加入することができる。顧客は、個人、組織、企業などの任意の実体であることができる。顧客がＣＳＰによって提供されたサービスに加入または登録するときに、その顧客のテナンシまたはアカウントが作成される。次に、顧客は、そのアカウントによって、アカウントに関連付けられた加入している１つまたは複数のクラウドリソースにアクセスすることができる。

【００２０】

前述したように、ＩａａＳ（infrastructure as a service）は、クラウドコンピューティングサービスの１つの特定の種類である。ＩａａＳモデルでは、ＣＳＰは、顧客自身のカスタマイズ可能なネットワークを構築し、顧客のリソースをデプロイするために顧客によって使用され得るインフラストラクチャ（クラウドサービスプロバイダインフラストラクチャまたはＣＳＰＩ（cloud services provider infrastructure）と呼ばれる）を提供する。したがって、顧客のリソースおよびネットワークは、ＣＳＰによって提供されたインフラストラクチャによって、分散環境内でホストされる。これは、顧客によって提供されたインフラストラクチャによって顧客のリソースおよびネットワークがホストされる従来のコンピューティングと異なっている。

【００２１】

ＣＳＰＩは、さまざまなホストマシン、メモリリソース、および基板ネットワークまたはアンダーレイネットワークとも呼ばれる物理ネットワークを形成するネットワークリソースを含む、相互接続された高性能な計算リソースを備えることができる。ＣＳＰＩにおけるリソースは、１つまたは複数の地理的領域にわたって地理的に分散され得る１つまたは複数のデータセンターにわたって分散されてよい。仮想化された分散環境を提供するために、これらの物理的リソースによって仮想化ソフトウェアが実行されてよい。この仮想化は、物理ネットワークの上にオーバーレイネットワーク（ソフトウェアベースネットワーク、ソフトウェア定義ネットワーク、または仮想ネットワークとしても知られている）を作成する。ＣＳＰＩの物理ネットワークは、１つまたは複数のオーバーレイネットワークまたは仮想ネットワークを物理ネットワークの上に作成するための基盤になる基礎を提供する。物理ネットワーク（または基板ネットワークもしくはアンダーレイネットワーク）は、物理的スイッチ、ルータ、コンピュータ、およびホストマシンなどの、物理ネットワークデバイスを含む。オーバーレイネットワークは、物理基板ネットワークの上で動作する論理（または仮想）ネットワークである。特定の物理ネットワークは、１つまたは複数のオーバーレイネットワークをサポートすることができる。オーバーレイネットワークは、通常、カプセル化技術を使用して、異なるオーバーレイネットワークに属するトラフィックを区別する。仮想ネットワークまたはオーバーレイネットワークは、仮想クラウドネットワーク（ＶＣＮ：virtual cloud network）とも呼ばれる。仮想ネットワークは、物理ネットワークの上で実行され得るネットワーク抽象化のレイヤを作成するために、ソフトウェア仮想化技術（例えば、ハイパーバイザ、ネットワーク仮想化デバイス（ＮＶＤ）（例えば、スマートＮＩＣ）、トップオブラック（ＴＯＲ：top-of-rack）スイッチ、ＮＶＤによって実行される１つまたは複数の機能を実施するスマートＴＯＲによって実施される仮想化機能、および他のメカニズム）を使用して実装される。仮想ネットワー

クは、ピアツーピアネットワーク、ＩＰネットワークなどを含む、多くの形態をとることができる。仮想ネットワークは、通常、レイヤ３　ＩＰネットワークまたはレイヤ２　ＶＬＡＮのいずれかである。仮想ネットワークまたはオーバーレイネットワークのこの方法は、多くの場合、仮想レイヤ３ネットワークまたはオーバーレイレイヤ３ネットワークと呼ばれる。仮想ネットワークのために開発されたプロトコルの例としては、ＩＰ－ｉｎ－ＩＰ（または汎用ルーティングカプセル化（ＧＲＥ：Generic Routing Encapsulation））仮想拡張可能ＬＡＮ（ＶＸＬＡＮ（Virtual Extensible LAN）－ＩＥＴＦ　ＲＦＣ　７３４８）、仮想プライベートネットワーク（ＶＰＮ：Virtual Private Networks）（例えば、ＭＰＬＳレイヤ３仮想プライベートネットワーク（ＲＦＣ　４３６４））、ＶＭｗａｒｅのＮＳＸ、ＧＥＮＥＶＥ（Generic Network Virtualization Encapsulation：汎用ネットワーク仮想化カプセル化）などが挙げられる。

【００２２】

ＩａａＳの場合、ＣＳＰによって提供されたインフラストラクチャ（ＣＳＰＩ）は、パブリックネットワーク（例えば、インターネット）を経由して仮想化されたコンピューティングリソースを提供するように構成され得る。ＩａａＳモデルでは、クラウドコンピューティングサービスプロバイダは、インフラストラクチャコンポーネント（例えば、サーバ、ストレージデバイス、ネットワークノード（例えば、ハードウェア）、デプロイメントソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザレイヤ）など）をホストすることができる。場合によっては、ＩａａＳプロバイダは、それらのインフラストラクチャコンポーネントに付随して生じるように、さまざまなサービス（例えば、請求書送付、監視、ロギング、セキュリティ、ロードバランシング、およびクラスタ化など）を提供してもよい。したがって、これらのサービスはポリシー主導であることができるため、ＩａａＳユーザは、ロードバランシングを駆動してアプリケーションの可用性および性能を維持するようにポリシーを実装することができてよい。ＣＳＰＩは、顧客が高度に利用可能なホストされた分散環境内で広範囲のアプリケーションおよびサービスを構築して実行できるようにする、インフラストラクチャおよび一連の補完するクラウドサービスを提供する。ＣＳＰＩは、顧客のオンプレミスネットワークからなど、さまざまなネットワーク化された場所から安全にアクセスできる柔軟な仮想ネットワーク内で、高性能な計算リソースおよび計算能力ならびにストレージ容量を提供する。顧客がＣＳＰによって提供されたＩａａＳサービスに加入または登録するときに、その顧客用に作成されるテナンシは、顧客が自分のクラウドリソースを作成、編成、および管理することができる、ＣＳＰＩ内の安全で分離されたパーティションである。

【００２３】

顧客は、ＣＳＰＩによって提供された計算リソース、メモリリソース、およびネットワークリソースを使用して、自分自身の仮想ネットワークを構築することができる。計算インスタンスなどの１つまたは複数の顧客のリソースまたはワークロードが、これらの仮想ネットワークにデプロイされ得る。例えば、顧客は、ＣＳＰＩによって提供されたリソースを使用して、仮想クラウドネットワーク（ＶＣＮ）と呼ばれる１つまたは複数のカスタマイズ可能なプライベート仮想ネットワークを構築することができる。顧客は、計算インスタンスなどの１つまたは複数の顧客のリソースを、顧客のＶＣＮにデプロイすることができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態をとることができる。したがって、ＣＳＰＩは、顧客が高度に利用可能なホストされた仮想環境内で広範囲のアプリケーションおよびサービスを構築して実行できるようにする、インフラストラクチャおよび一連の補完するクラウドサービスを提供する。顧客は、ＣＳＰＩによって提供された基盤になる物理的リソースを管理することも制御することもないが、オペレーティングシステム、ストレージ、デプロイされたアプリケーションを制御することができ、場合によっては、選ばれたネットワークコンポーネント（例えば、ファイアウォール）を限定的に制御することができる。

【００２４】

ＣＳＰは、顧客およびネットワーク管理者が、ＣＳＰＩリソースを使用してクラウド内

でデプロイされたリソースの構成、アクセス、および管理を行うことを可能にする、コンソールを提供してよい。ある実施形態では、このコンソールは、ＣＳＰＩにアクセスして管理するために使用され得るＷｅｂベースのユーザインターフェイスを提供する。一部の実装では、コンソールは、ＣＳＰによって提供されたＷｅｂベースのアプリケーションである。

【００２５】

ＣＳＰＩは、シングルテナンシアーキテクチャまたはマルチテナンシアーキテクチャをサポートしてよい。シングルテナンシアーキテクチャでは、ソフトウェアコンポーネント（例えば、アプリケーション、データベース）またはハードウェアコンポーネント（例えば、ホストマシンまたはサーバ）が、単一の顧客またはテナントのために働く。マルチテナンシアーキテクチャでは、ソフトウェアコンポーネントまたはハードウェアコンポーネントは、複数の顧客またはテナントのために働く。したがって、マルチテナンシアーキテクチャでは、ＣＳＰＩリソースは、複数の顧客またはテナント間で共有される。マルチテナンシの状況では、各テナントのデータが分離され、他のテナントには見えないままであることを保証するために、予防策が取られ、ＣＳＰＩ内に予防手段が導入される。

【００２６】

物理ネットワークでは、ネットワークエンドポイント（「エンドポイント」）は、物理ネットワークに接続され、接続先のネットワークとの間で通信するコンピューティングデバイスまたはシステムのことを指す。物理ネットワーク内のネットワークエンドポイントは、ローカルエリアネットワーク（ＬＡＮ：Local Area Network）、広域ネットワーク（ＷＡＮ：Wide Area Network）、または他の種類の物理ネットワークに接続されてよい。物理ネットワーク内の従来のエンドポイントの例としては、モデム、ハブ、ブリッジ、スイッチ、ルータ、および他のネットワークデバイス、物理コンピュータ（またはホストマシン）などが挙げられる。物理ネットワーク内の各物理デバイスは、デバイスと通信するために使用され得る固定ネットワークアドレスを有する。この固定ネットワークアドレスは、レイヤ２アドレス（例えば、ＭＡＣアドレス）、固定レイヤ３アドレス（例えば、ＩＰアドレス）などであることができる。仮想環境または仮想ネットワークでは、エンドポイントは、物理ネットワークのコンポーネントによってホストされる（例えば、物理ホストマシンによってホストされる）仮想マシンなどの、さまざまな仮想エンドポイントを含むことができる。仮想ネットワーク内のこれらのエンドポイントは、オーバーレイレイヤ２アドレス（例えば、オーバーレイＭＡＣアドレス）およびオーバーレイレイヤ３アドレス（例えば、オーバーレイＩＰアドレス）などのオーバーレイアドレスによってアドレス指定される。ネットワークオーバーレイは、ネットワーク管理者がソフトウェア管理を使用して（例えば、仮想ネットワークの制御プレーンを実装するソフトウェアによって）ネットワークエンドポイントに関連付けられたオーバーレイアドレス間を移動できるようにすることによって、柔軟性を可能にする。したがって、物理ネットワークとは異なり、仮想ネットワークでは、ネットワーク管理ソフトウェアを使用して、オーバーレイアドレス（例えば、オーバーレイＩＰアドレス）が１つのエンドポイントから別のエンドポイントに移動され得る。仮想ネットワークが物理ネットワークの上に構築されるため、仮想ネットワーク内のコンポーネント間の通信は、仮想ネットワークおよび基盤になる物理ネットワークの両方を含む。そのような通信を容易にするために、ＣＳＰＩのコンポーネントは、仮想ネットワーク内のオーバーレイアドレスを基板ネットワーク内の実際の物理アドレスに、およびその逆に、マッピングするマッピングを学習して格納するように構成される。その後、これらのマッピングは、通信を容易にするために使用される。顧客トラフィックは、仮想ネットワーク内のルーティングを容易にするためにカプセル化される。

【００２７】

したがって、物理アドレス（例えば、物理ＩＰアドレス）は、物理ネットワーク内のコンポーネントに関連付けられ、オーバーレイアドレス（例えば、オーバーレイＩＰアドレス）は、仮想ネットワークまたはオーバーレイネットワーク内の実体に関連付けられる。

物理ＩＰアドレスは、基板ネットワークまたは物理ネットワーク内の物理デバイス（例えば、ネットワークデバイス）に関連付けられたＩＰアドレスである。例えば、各ＮＶＤは、関連付けられた物理ＩＰアドレスを有する。オーバーレイＩＰアドレスは、顧客の仮想クラウドネットワーク（ＶＣＮ）内の計算インスタンスに関連付けられるなど、オーバーレイネットワーク内の実体に関連付けられたオーバーレイアドレスである。自分自身のプライベートＶＣＮを各々有する２つの異なる顧客またはテナントは、互いについての知識を何も持たずに、それらのＶＣＮ内で同じオーバーレイＩＰアドレスを使用できる可能性がある。物理ＩＰアドレスおよびオーバーレイＩＰアドレスは、両方とも、実ＩＰアドレスの種類である。これらのＩＰアドレスは、仮想ＩＰアドレスとは別に存在する。仮想ＩＰアドレスは、通常、複数の実ＩＰアドレスを表すか、または複数の実ＩＰアドレスにマッピングされる、単一のＩＰアドレスである。仮想ＩＰアドレスは、仮想ＩＰアドレスと複数の実ＩＰアドレスの間の１対多のマッピングを提供する。例えば、ロードバランサは、ＶＩＰを使用して、複数のサーバにマッピングされるか、または複数のサーバを表してよく、各サーバは、それ自身の実ＩＰアドレスを有する。

【００２８】

クラウドインフラストラクチャまたはＣＳＰＩは、世界中の１つまたは複数のリージョンの１つまたは複数のデータセンター内で、物理的にホストされる。ＣＳＰＩは、物理ネットワークまたは基板ネットワーク内のコンポーネント、および物理ネットワークのコンポーネントの上に構築された仮想ネットワーク内にある仮想コンポーネント（例えば、仮想ネットワーク、計算インスタンス、仮想マシンなど）を含んでよい。ある実施形態では、ＣＳＰＩは、レルム、リージョン、および可用性ドメイン内で編成され、ホストされる。リージョンは、通常、１つまたは複数のデータセンターを含む局所的な地理的領域である。リージョンは、一般に、互いに独立しており、例えば、複数の国または大陸にわたる広大な距離によって分離され得る。例えば、第１のリージョンがオーストラリアにあってよく、別のリージョンが日本にあってよく、さらに別のリージョンがインドにあってよい、などである。各リージョンがＣＳＰＩリソースのそのリージョン自体の独立したサブセットを含むように、ＣＳＰＩリソースがリージョン間で分割される。各リージョンは、計算リソース（例えば、ベアメタルサーバ、仮想マシン、コンテナ、および関連するインフラストラクチャなど）、ストレージリソース（例えば、ブロックボリュームストレージ、ファイルストレージ、オブジェクトストレージ、アーカイブストレージ）、ネットワークリソース（例えば、仮想クラウドネットワーク（ＶＣＮ）、ロードバランシングリソース、オンプレミスネットワークへの接続）、データベースリソース、エッジネットワークリソース（例えば、ＤＮＳ）、ならびにアクセス管理および監視リソースなどの、一連のコアインフラストラクチャサービスおよびリソースを提供してよい。各リージョンは、一般に、レルム内の他のリージョンに接続する複数の経路を有する。

【００２９】

近くのリソースを使用することが、遠いリソースを使用することよりも高速であるため、一般にアプリケーションは、そのアプリケーションが最も頻繁に使用されるリージョン内でデプロイされる（すなわち、そのリージョンに関連付けられたインフラストラクチャにデプロイされる）。アプリケーションは、大きい気象系または地震などのリージョン全体のイベントのリスクを軽減すること、法律管轄区域、税領域に関する変化する要件、および他のビジネス上の基準または社会的基準を満たすことなどのための冗長性などの、さまざまな理由で、異なるリージョン内でデプロイされることも可能である。

【００３０】

リージョン内のデータセンターは、可用性ドメイン（ＡＤ：availability domains）にさらに編成されて細分化され得る。可用性ドメインは、リージョン内に位置する１つまたは複数のデータセンターに対応してよい。リージョンは、１つまたは複数の可用性ドメインで構成され得る。そのような分散環境では、ＣＳＰＩリソースは、仮想クラウドネットワーク（ＶＣＮ）など、リージョンに固有であるか、または計算インスタンスなど、可用性ドメインに固有である。

【００３１】
リージョン内のＡＤは、互いに分離され、故障耐性があり、同時に故障する可能性が極めて低くなるように構成される。これは、リージョン内の１つのＡＤでの故障が同じリージョン内の他のＡＤの可用性に影響を与える可能性が低くなるように、ネットワーク、物理ケーブル、ケーブル経路、ケーブルエントリポイントなどの重要なインフラストラクチャリソースを共有しないＡＤによって実現される。同じリージョン内のＡＤは、高可用性接続を他のネットワーク（例えば、インターネット、顧客のオンプレミスネットワークなど）に提供すること、ならびに高可用性および災害復旧の両方のために複数のＡＤ内に複製されたシステムを構築することを可能にする、待ち時間の短い高帯域幅ネットワークによって互いに接続されてよい。クラウドサービスは、複数のＡＤを使用して高可用性を保証し、リソースの故障に対して保護する。ＩａａＳプロバイダによって提供されたインフラストラクチャが増大するにつれて、追加の能力を有するより多くのリージョンおよびＡＤが追加されてよい。可用性ドメイン間のトラフィックは、通常、暗号化される。
【００３２】
ある実施形態では、リージョンは、レルムにグループ化される。レルムは、リージョンの論理的集合である。レルムは、互いに分離され、どのデータも共有しない。同じレルム内のリージョンは、互いに通信してよいが、異なるレルム内のリージョンは通信することができない。顧客のテナンシまたはアカウントは、ＣＳＰと共に、単一のレルム内に存在し、そのレルムに属する１つまたは複数のリージョンにわたって分散され得る。通常、顧客がＩａａＳサービスに加入するときに、レルム内の顧客によって指定されたリージョン（「ホーム」リージョンと呼ばれる）内に、その顧客用のテナンシまたはアカウントが作成される。顧客は、レルム内の１つまたは複数の他のリージョンにわたって顧客のテナンシを拡張することができる。顧客は、顧客のテナンシが存在するレルム内にないリージョンにアクセスすることができない。
【００３３】
ＩａａＳプロバイダは、複数のレルムを提供することができ、各レルムは、顧客またはユーザの特定のセットの要求に応じる。例えば、商用レルムは、商業の顧客に提供されてよい。別の例として、レルムは、ある国の中の顧客のために、その特定の国に提供されてよい。さらに別の例として、政府レルムが政府などに提供されてよい。例えば、政府レルムは、特定の政府の要求に応じてよく、商用レルムより高度なセキュリティを有してよい。例えば、Oracleクラウドインフラストラクチャ（ＯＣＩ）は、商用リージョンのためのレルムおよび政府クラウドリージョンのための（例えば、FedRAMP認定およびＩＬ５認定の）２つのレルムを現在提供している。
【００３４】
ある実施形態では、ＡＤは、１つまたは複数の障害ドメインに細分化され得る。障害ドメインは、アンチアフィニティを提供するためのＡＤ内のインフラストラクチャリソースのグループである。障害ドメインは、複数の計算インスタンスが単一のＡＤ内の同じ物理ハードウェア上に存在しないように、計算インスタンスの分散を可能にする。この分散は、アンチアフィニティとして知られている。障害ドメインは、単一障害点を共有するハードウェアコンポーネント（コンピュータ、スイッチなど）のセットのことを指す。計算プールが、障害ドメインに論理的に分割される。そのため、１つの障害ドメインに影響を与えるハードウェア故障または計算ハードウェアの保守イベントが、他の障害ドメイン内のインスタンスに影響を与えない。実施形態に応じて、ＡＤごとの障害ドメインの数は変わってよい。例えば、ある実施形態では、各ＡＤは３つの障害ドメインを含む。障害ドメインは、ＡＤ内の論理データセンターとして機能する。
【００３５】
顧客がＩａａＳサービスに加入するときに、ＣＳＰＩからのリソースが、顧客のためにプロビジョニングされ、顧客のテナンシに関連付けられる。顧客は、これらのプロビジョニングされたリソースを使用して、プライベートネットワークを構築し、リソースをこれらのネットワークにデプロイすることができる。ＣＳＰＩによってクラウド内でホストさ

れている顧客のネットワークは、仮想クラウドネットワーク（ＶＣＮ）と呼ばれる。顧客は、顧客に割り当てられているＣＳＰＩリソースを使用して、１つまたは複数の仮想クラウドネットワーク（ＶＣＮ）を設定することができる。ＶＣＮは、仮想プライベートネットワークまたはソフトウェア定義プライベートネットワークである。顧客のＶＣＮ内でデプロイされている顧客のリソースは、計算インスタンス（例えば、仮想マシン、ベアメタルインスタンス）および他のリソースを含むことができる。これらの計算インスタンスは、アプリケーション、ロードバランサ、データベースなどの、さまざまな顧客のワークロードを表してよい。ＶＣＮにデプロイされた計算インスタンスは、インターネットなどのパブリックネットワークを経由してパブリックにアクセスできるエンドポイント（「パブリックエンドポイント」）と、同じＶＣＮまたは他のＶＣＮ（例えば、顧客の他のＶＣＮ、または顧客に属していないＶＣＮ）内の他のインスタンスと、顧客のオンプレミスのデータセンターまたはネットワークと、ならびにサービスエンドポイントおよび他の種類のエンドポイントと、通信することができる。

【００３６】

ＣＳＰは、ＣＳＰＩを使用してさまざまなサービスを提供してよい。場合によっては、ＣＳＰＩの顧客は、自分自身がサービスプロバイダのように振る舞い、ＣＳＰＩリソースを使用してサービスを提供してよい。サービスプロバイダは、識別情報（例えば、ＩＰアドレス、ＤＮＳ名、およびＤＮＳポート）によって特徴付けられたサービスエンドポイントを公開してよい。顧客のリソース（例えば、計算インスタンス）は、特定のサービスのためにサービスによって公開されたサービスエンドポイントにアクセスすることによって、その特定のサービスを消費することができる。これらのサービスエンドポイントは、一般に、インターネットなどのパブリック通信ネットワークを介して、エンドポイントに関連付けられたパブリックＩＰアドレスを使用してユーザによってパブリックにアクセスできるエンドポイントである。パブリックにアクセスできるネットワークエンドポイントは、パブリックエンドポイントと呼ばれることもある。

【００３７】

ある実施形態では、サービスプロバイダは、サービスのためのエンドポイント（サービスエンドポイントと呼ばれることがある）を介してサービスを公開してよい。次に、サービスの顧客は、このサービスエンドポイントを使用してサービスにアクセスすることができる。ある実装では、サービスのために提供されたサービスエンドポイントは、そのサービスを消費しようとする複数の顧客によってアクセスされ得る。他の実装では、専用サービスエンドポイントが顧客に提供されてよく、その客のみが、その専用サービスエンドポイントを使用してサービスにアクセスできるようにする。

【００３８】

ある実施形態では、ＶＣＮが作成されるときに、そのＶＣＮは、ＶＣＮに割り当てられているプライベートオーバーレイＩＰアドレスの範囲（例えば、１０．０／１６）である、プライベートオーバーレイクラスレスドメイン間ルーティング（ＣＩＤＲ：Classless Inter-Domain Routing）アドレス空間に関連付けられる。ＶＣＮは、関連付けられたサブネット、ルートテーブル、およびゲートウェイを含む。ＶＣＮは、単一のリージョン内に存在するが、リージョンの可用性ドメインのうちの１つまたは複数あるいはすべてに及ぶことができる。ゲートウェイは、ＶＣＮのために構成されている仮想インターフェイスであり、ＶＣＮとの間で、ＶＣＮの外側の１つまたは複数のエンドポイントへのトラフィックの通信を可能にする。異なる種類のエンドポイントとの間での通信を可能にするために、ＶＣＮのための１つまたは複数の異なる種類のゲートウェイが構成されてよい。

【００３９】

ＶＣＮは、１つまたは複数のサブネットなどの１つまたは複数のサブネットワークに細分化され得る。したがって、サブネットは、ＶＣＮ内で作成され得る構成または細分化の単位である。ＶＣＮは、１つまたは複数のサブネットを含むことができる。ＶＣＮ内の各サブネットは、そのＶＣＮ内の他のサブネットと重複しない、ＶＣＮのアドレス空間内のアドレス空間サブセットを表す、オーバーレイＩＰアドレスの連続的な範囲（例えば、１

０．０．０．０／２４および１０．０．１．０／２４）に関連付けられる。

【００４０】

各計算インスタンスは、計算インスタンスがＶＣＮのサブネットに参加できるようにする仮想ネットワークインターフェイスカード（ＶＮＩＣ：virtual network interface card）に関連付けられる。ＶＮＩＣは、物理ネットワークインターフェイスカード（ＮＩＣ：Network Interface Card）の論理的表現である。一般に、ＶＮＩＣは、実体（例えば、計算インスタンス、サービス）と仮想ネットワークの間のインターフェイスである。ＶＮＩＣは、サブネットに存在し、１つまたは複数の関連付けられたＩＰアドレス、および関連付けられたセキュリティルールまたはセキュリティポリシーを有する。ＶＮＩＣは、スイッチ上のレイヤ２ポートと同等である。ＶＮＩＣは、計算インスタンスに接続され、ＶＣＮ内のサブネットに接続される。計算インスタンスに関連付けられたＶＮＩＣは、計算インスタンスが、ＶＣＮのサブネットの一部になることを可能にし、計算インスタンスが、計算インスタンスと同じサブネット上にあるエンドポイントと、ＶＣＮ内の異なるサブネット内のエンドポイントと、またはＶＣＮの外側のエンドポイントと、通信する（例えば、パケットを送信および受信する）ことを可能にする。したがって、計算インスタンスに関連付けられたＶＮＩＣは、計算インスタンスがＶＣＮの内側および外側のエンドポイントと接続する方法を決定する。計算インスタンスのためのＶＮＩＣは、計算インスタンスが作成されてＶＣＮ内のサブネットに追加されるときに、作成されてその計算インスタンスに関連付けられる。計算インスタンスのセットを含んでいるサブネットの場合、サブネットは、計算インスタンスのセットに対応するＶＮＩＣを含み、各ＶＮＩＣは、計算インスタンスのセット内の１つの計算インスタンスに接続される。

【００４１】

各計算インスタンスには、計算インスタンスに関連付けられたＶＮＩＣを介して、プライベートオーバーレイＩＰアドレスが割り当てられる。このプライベートオーバーレイＩＰアドレスは、計算インスタンスが作成されるときに、計算インスタンスに関連付けられたＶＮＩＣに割り当てられ、計算インスタンスとの間でトラフィックをルーティングするために使用される。特定のサブネット内のすべてのＶＮＩＣは、同じルートテーブル、セキュリティリスト、およびＤＨＣＰオプションを使用する。前述したように、ＶＣＮ内の各サブネットは、そのＶＣＮ内の他のサブネットと重複しない、ＶＣＮのアドレス空間内のアドレス空間サブセットを表す、オーバーレイＩＰアドレスの連続的な範囲（例えば、１０．０．０．０／２４および１０．０．１．０／２４）に関連付けられる。ＶＣＮの特定のサブネット上のＶＮＩＣの場合、ＶＮＩＣに割り当てられているプライベートオーバーレイＩＰアドレスは、このサブネットに割り当てられたオーバーレイＩＰアドレスの連続的な範囲からのアドレスである。

【００４２】

ある実施形態では、計算インスタンスには、任意選択的に、プライベートオーバーレイＩＰアドレスに加えて、例えば、パブリックサブネット内である場合、１つまたは複数のパブリックＩＰアドレスなどの、追加のオーバーレイＩＰアドレスが割り当てられてよい。これらの複数のアドレスは、同じＶＮＩＣに割り当てられるか、または計算インスタンスに関連付けられている複数のＶＮＩＣにわたって割り当てられる。しかし、各インスタンスは、インスタンスの起動中に作成され、インスタンスに割り当てられたプライベートオーバーレイＩＰアドレスに関連付けられる、プライマリＶＮＩＣを有し、このプライマリＶＮＩＣは除去され得ない。セカンダリＶＮＩＣと呼ばれる追加のＶＮＩＣが、プライマリＶＮＩＣと同じ可用性ドメイン内の既存のインスタンスに追加され得る。すべてのＶＮＩＣは、インスタンスと同じ可用性ドメイン内にある。セカンダリＶＮＩＣは、プライマリＶＮＩＣと同じＶＣＮ内のサブネット内、または同じＶＣＮ内もしくは異なるＶＣＮ内のいずれかにある異なるサブネット内にあることができる。

【００４３】

計算インスタンスがパブリックサブネット内にある場合、計算インスタンスには、任意選択的に、パブリックＩＰアドレスが割り当てられてよい。サブネットが作成されるとき

に、サブネットは、パブリックサブネットまたはプライベートサブネットのいずれかとして指定され得る。プライベートサブネットは、サブネット内のリソース（例えば、計算インスタンス）および関連付けられたＶＮＩＣがパブリックオーバーレイＩＰアドレスを有することができないということを意味する。パブリックサブネットは、サブネット内のリソースおよび関連付けられたＶＮＩＣがパブリックＩＰアドレスを有することができるということを意味する。顧客は、単一の可用性ドメイン内に存在するか、またはリージョン内もしくはレルム内の複数の可用性ドメインにわたって存在するように、サブネットを指定することができる。

【００４４】

前述したように、ＶＣＮは、１つまたは複数のサブネットに細分化されてよい。ある実施形態では、ＶＣＮのために構成された仮想ルータ（ＶＲ：Virtual Router）（ＶＣＮ ＶＲまたは単にＶＲと呼ばれる）が、ＶＣＮのサブネット間の通信を可能にする。ＶＣＮ内のサブネットの場合、ＶＲは、そのサブネットの論理ゲートウェイを表し、サブネット（すなわち、そのサブネット上の計算インスタンス）が、ＶＣＮ内の他のサブネット上のエンドポイントと、およびＶＣＮの外側の他のエンドポイントと、通信できるようにする。ＶＣＮ　ＶＲは、ＶＣＮ内のＶＮＩＣとＶＣＮに関連付けられた仮想ゲートウェイ（「ゲートウェイ」）の間のトラフィックをルーティングするように構成された論理的実体である。ゲートウェイは、図１に関して下でさらに説明される。ＶＣＮ　ＶＲは、レイヤ３／ＩＰレイヤの概念である。１つの実施形態では、１つのＶＣＮに対して１つのＶＣＮ ＶＲが存在し、ＶＣＮ　ＶＲは、場合によっては、ＩＰアドレスによってアドレス指定される無制限の数のポートを有し、ＶＣＮのサブネットごとに１つのポートがある。このようにして、ＶＣＮ　ＶＲは、ＶＣＮ　ＶＲが接続されたＶＣＮ内のサブネットごとに異なるＩＰアドレスを有する。ＶＲは、ＶＣＮのために構成されたさまざまなゲートウェイにも接続される。ある実施形態では、サブネットのオーバーレイＩＰアドレス範囲からの特定のオーバーレイＩＰアドレスが、そのサブネットのＶＣＮ　ＶＲのポートのために予約されている。例えば、関連付けられたアドレス範囲１０．０／１６および１０．１／１６をそれぞれ有する２つのサブネットを含んでいるＶＣＮについて考える。アドレス範囲１０．０／１６を有するＶＣＮ内の第１のサブネットの場合、この範囲からのアドレスが、そのサブネットのＶＣＮ　ＶＲのポートのために予約されている。場合によっては、この範囲からの最初のＩＰアドレスが、ＶＣＮ　ＶＲのために予約されてよい。例えば、オーバーレイＩＰアドレス範囲１０．０／１６を有するサブネットの場合、ＩＰアドレス１０．０．０．１が、そのサブネットのＶＣＮ　ＶＲのポートのために予約されてよい。アドレス範囲１０．１／１６を有する同じＶＣＮ内の第２のサブネットの場合、ＶＣＮ　ＶＲは、ＩＰアドレス１０．１．０．１を有するその第２のサブネットのポートを有してよい。ＶＣＮ ＶＲは、ＶＣＮ内のサブネットの各々について、異なるＩＰアドレスを有する。

【００４５】

一部の他の実施形態では、ＶＣＮ内の各サブネットは、ＶＲに関連付けられた予約されたＩＰアドレスまたはデフォルトのＩＰアドレスを使用してサブネットによってアドレス指定可能である、それ自体に関連付けられたＶＲを含んでよい。予約されたＩＰアドレスまたはデフォルトのＩＰアドレスは、例えば、そのサブネットに関連付けられたＩＰアドレスの範囲からの最初のＩＰアドレスであってよい。サブネット内のＶＮＩＣは、このデフォルトのＩＰアドレスまたは予約されたＩＰアドレスを使用して、サブネットに関連付けられたＶＲと通信する（例えば、パケットを送信および受信する）ことができる。そのような実施形態では、ＶＲは、そのサブネットの入口／出口ポイントである。ＶＣＮ内のサブネットに関連付けられたＶＲは、ＶＣＮ内の他のサブネットに関連付けられた他のＶＲと通信することができる。ＶＲは、ＶＣＮに関連付けられたゲートウェイと通信することもできる。サブネットのＶＲ機能は、サブネット内のＶＮＩＣのＶＮＩＣ機能を実行している１つまたは複数のＮＶＤ上で動作しているか、または１つまたは複数のＮＶＤによって実行される。

【００４６】

ルートテーブル、セキュリティルール、およびＤＨＣＰオプションが、ＶＣＮのために構成されてよい。ルートテーブルは、ＶＣＮの仮想ルートテーブルであり、ゲートウェイまたは特別に構成されたインスタンスを経由してＶＣＮ内のサブネットからＶＣＮの外側の送信先へトラフィックをルーティングするためのルールを含む。ＶＣＮのルートテーブルは、ＶＣＮとの間でパケットが転送／ルーティングされる方法を制御するようにカスタマイズされ得る。ＤＨＣＰオプションは、インスタンスが起動するときにインスタンスに自動的に提供される構成情報のことを指す。

【００４７】

ＶＣＮのために構成されたセキュリティルールは、ＶＣＮのオーバーレイファイアウォールルールを表す。セキュリティルールは、入口ルールおよび出口ルールを含み、ＶＣＮ内のインスタンスの内外に許可される（例えば、プロトコルおよびポートに基づく）トラフィックの種類を指定することができる。顧客は、特定のルールがステートフルであるか、またはステートレスであるかを選択することができる。例えば、顧客は、送信元ＣＩＤＲ０．０．０．０／０および送信先ＴＣＰポート２２を含むステートフル入口ルールを設定することによって、任意の位置からインスタンスのセットへの着信ＳＳＨトラフィックを許可することができる。ネットワークセキュリティグループまたはセキュリティリストを使用して、セキュリティルールが実装され得る。ネットワークセキュリティグループは、そのグループ内のリソースのみに当てはまるセキュリティルールのセットで構成される。一方、セキュリティリストは、セキュリティリストを使用する任意のサブネット内のすべてのリソースに当てはまるルールを含む。ＶＣＮは、デフォルトのセキュリティルールを含むデフォルトのセキュリティリストを備えてよい。ＶＣＮのために構成されたＤＨＣＰオプションは、インスタンスが起動するときにＶＣＮ内のインスタンスに自動的に提供される構成情報を提供する。

【００４８】

ある実施形態では、ＶＣＮの構成情報は、ＶＣＮ制御プレーンによって決定されて格納される。ＶＣＮの構成情報は、例えば、ＶＣＮに関連付けられたアドレス範囲に関する情報、ＶＣＮ内のサブネットおよび関連付けられた情報、ＶＣＮに関連付けられた１つまたは複数のＶＲ、ＶＣＮ内の計算インスタンスおよび関連付けられたＶＮＩＣ、ＶＣＮに関連付けられたさまざまな仮想化ネットワーク機能を実行するＮＶＤ（例えば、ＶＮＩＣ、ＶＲ、ゲートウェイ）、ＶＣＮの状態情報、ならびに他のＶＣＮに関連する情報を含んでよい。ある実施形態では、ＶＣＮ配布サービスが、ＶＣＮ制御プレーンまたはその一部によって格納された構成情報をＮＶＤに公開する。配布された情報は、パケットをＶＣＮ内の計算インスタンスとの間で転送するためにＮＶＤによって格納されて使用される情報（例えば、転送テーブル、ルーティングテーブルなど）を更新するために使用されてよい。

【００４９】

ある実施形態では、ＶＣＮおよびサブネットの作成は、ＶＣＮ制御プレーン（ＣＰ：Ｃontrol Plane）によって処理され、計算インスタンスの起動は、計算制御プレーンによって処理される。計算制御プレーンは、物理的リソースを計算インスタンスに割り当てる役割を担い、その後、ＶＣＮ制御プレーンを呼び出してＶＮＩＣを作成し、計算インスタンスに接続する。ＶＣＮ　ＣＰは、ＶＣＮデータマッピングも、パケット転送およびルーティング機能を実行するように構成されたＶＣＮデータプレーンに送信する。ある実施形態では、ＶＣＮ　ＣＰは、更新をＶＣＮデータプレーンに提供する役割を担う配布サービスを提供する。ＶＣＮ制御プレーンの例が、図６、図７、図８、および図９にも示されており（参照番号６１６、７１６、８１６、および９１６を参照）、下で説明される。

【００５０】

顧客は、ＣＳＰＩによってホストされたリソースを使用して、１つまたは複数のＶＣＮを作成してよい。顧客のＶＣＮにデプロイされた計算インスタンスは、さまざまなエンドポイントと通信してよい。これらのエンドポイントは、ＣＳＰＩによってホストされているエンドポイント、およびＣＳＰＩの外側のエンドポイントを含むことができる。

【００５１】

ＣＳＰＩを使用してクラウドベースのサービスを実装するためのさまざまな異なるアーキテクチャが、図１、図２、図３、図４、図５、および図１８～図２２に示されており、下で説明される。図１は、ある実施形態によるＣＳＰＩによってホストされたオーバーレイＶＣＮまたは顧客のＶＣＮを示す分散環境１００の高レベルの図である。図１に示された分散環境は、オーバーレイネットワーク内に複数のコンポーネントを含む。図１に示された分散環境１００は、単に例であり、主張される実施形態の範囲を過度に限定するよう意図されていない。多くの変形、代替手段、および変更が可能である。例えば、一部の実装では、図１に示された分散環境は、図１に示されたシステムまたはコンポーネントより多いか、または少ないシステムまたはコンポーネントを含んでよく、２つ以上のサブシステムを組み合わせてよく、またはシステムの異なる構成もしくは配置を含んでよい。

【００５２】

図１に示された例に示されているように、分散環境１００は、顧客が加入し、自分の仮想クラウドネットワーク（ＶＣＮ）を構築するために使用できるサービスおよびリソースを提供するＣＳＰＩ１０１を含む。ある実施形態では、ＣＳＰＩ１０１は、ＩａａＳサービスを加入している顧客に提供する。ＣＳＰＩ１０１内のデータセンターは、１つまたは複数のリージョンに編成されてよい。１つの例示的なリージョン「リージョンＵＳ」１０２が、図１に示されている。顧客は、リージョン１０２に関して、Oracle International Corporationの顧客のＶＣＮを構成している。顧客は、さまざまな計算インスタンスをＶＣＮ１０４にデプロイしてよく、計算インスタンスは、仮想マシンまたはベアメタルインスタンスを含んでよい。インスタンスの例としては、アプリケーション、データベース、ロードバランサなどが挙げられる。

【００５３】

図１に示された実施形態では、顧客のＶＣＮ１０４は、２つのサブネット、すなわち、「サブネット１」および「サブネット２」を含み、各サブネットは、それ自体のＣＩＤＲＩＰアドレス範囲を有する。図１では、サブネット１のオーバーレイＩＰアドレス範囲が１０．０／１６であり、サブネット２のアドレス範囲が１０．１／１６である。ＶＣＮ仮想ルータ１０５は、ＶＣＮ１０４のサブネット間およびＶＣＮの外側の他のエンドポイントとの通信を可能にする、ＶＣＮの論理ゲートウェイを表す。ＶＣＮ　ＶＲ１０５は、ＶＣＮ１０４内のＶＮＩＣとＶＣＮ１０４に関連付けられたゲートウェイの間のトラフィックをルーティングするように構成される。ＶＣＮ　ＶＲ１０５は、ＶＣＮ１０４のサブネットごとにポートを提供する。例えば、ＶＲ１０５は、サブネット１のＩＰアドレス１０．０．０．１を有するポートおよびサブネット２のＩＰアドレス１０．１．０．１を有するポートを提供してよい。

【００５４】

複数の計算インスタンスが各サブネットにデプロイされてよく、計算インスタンスは、仮想マシンインスタンスおよび／またはベアメタルインスタンスであることができる。サブネット内の計算インスタンスは、ＣＳＰＩ１０１内の１つまたは複数のホストマシンによってホストされてよい。計算インスタンスは、計算インスタンスに関連付けられたＶＮＩＣを介してサブネットに参加する。例えば、図１に示されているように、計算インスタンスＣ１は、この計算インスタンスに関連付けられたＶＮＩＣを介してサブネット１の一部になる。同様に、計算インスタンスＣ２は、Ｃ２に関連付けられたＶＮＩＣを介してサブネット１の一部になる。同様の方法で、仮想マシンインスタンスまたはベアメタルインスタンスであってよい複数の計算インスタンスが、サブネット１の一部になってよい。各計算インスタンスには、それに関連付けられたＶＮＩＣを介して、プライベートオーバーレイＩＰアドレスおよびＭＡＣアドレスが割り当てられる。例えば、図１では、計算インスタンスＣ１は、１０．０．０．２のオーバーレイＩＰアドレスおよびＭ１のＭＡＣアドレスを有し、一方、計算インスタンスＣ２は、１０．０．０．３のプライベートオーバーレイＩＰアドレスおよびＭ２のＭＡＣアドレスを有する。計算インスタンスＣ１およびＣ２を含むサブネット１内の各計算インスタンスは、サブネット１のＶＣＮ　ＶＲ１０５のポートのＩＰアドレスであるＩＰアドレス１０．０．０．１を使用するＶＣＮ　ＶＲ１０

５へのデフォルトのルートを有する。
【００５５】
サブネット２には、仮想マシンインスタンスおよび／またはベアメタルインスタンスを含む、複数の計算インスタンスがデプロイされ得る。例えば、図１に示されているように、計算インスタンスＤ１およびＤ２は、それぞれの計算インスタンスに関連付けられたＶＮＩＣを介してサブネット２の一部になる。図１に示された実施形態では、計算インスタンスＤ１は、１０．１．０．２のオーバーレイＩＰアドレスおよびＭＭ１のＭＡＣアドレスを有し、一方、計算インスタンスＤ２は、１０．１．０．３のプライベートオーバーレイＩＰアドレスおよびＭＭ２のＭＡＣアドレスを有する。計算インスタンスＤ１およびＤ２を含むサブネット２内の各計算インスタンスは、サブネット２のＶＣＮ　ＶＲ１０５のポートのＩＰアドレスであるＩＰアドレス１０．１．０．１を使用するＶＣＮ　ＶＲ１０５へのデフォルトのルートを有する。
【００５６】
ＶＣＮ　Ａ１０４は、１つまたは複数のロードバランサを含んでもよい。例えば、ロードバランサは、サブネットに提供されてよく、サブネット上の複数の計算インスタンスにわたってトラフィックをロードバランスするように構成されてよい。ロードバランサは、ＶＣＮ内の複数のサブネットにわたってトラフィックをロードバランスするために提供されてもよい。
【００５７】
ＶＣＮ１０４にデプロイされた特定の計算インスタンスは、さまざまなエンドポイントと通信することができる。これらのエンドポイントは、ＣＳＰＩ２００によってホストされているエンドポイント、およびＣＳＰＩ２００の外側のエンドポイントを含んでよい。ＣＳＰＩ１０１によってホストされているエンドポイントは、特定の計算インスタンスと同じサブネット上のエンドポイント（例えば、サブネット１内の２つの計算インスタンス間の通信）、異なるサブネット上の、ただし同じＶＣＮ内のエンドポイント（例えば、サブネット１内の計算インスタンスとサブネット２内の計算インスタンスとの間の通信）、同じリージョン内の異なるＶＣＮ内のエンドポイント（例えば、サブネット１内の計算インスタンスと同じリージョン１０６または１１０内のＶＣＮ内のエンドポイントとの間の通信、サブネット１内の計算インスタンスと同じリージョン内のサービスネットワーク１１０内のエンドポイントとの間の通信）、または異なるリージョン内のＶＣＮ内のエンドポイント（例えば、サブネット１内の計算インスタンスと異なるリージョン１０８内のＶＣＮ内のエンドポイントとの間の通信）を含んでよい。ＣＳＰＩ１０１によってホストされたサブネット内の計算インスタンスは、ＣＳＰＩ１０１によってホストされていない（すなわち、ＣＳＰＩ１０１の外側にある）エンドポイントと通信してもよい。これらの外側のエンドポイントは、顧客のオンプレミスネットワーク１１６内のエンドポイント、他のリモートクラウドによってホストされたネットワーク１１８内のエンドポイント、インターネットなどのパブリックネットワークを介してアクセス可能なパブリックエンドポイント１１４、および他のエンドポイントを含む。
【００５８】
同じサブネット上の計算インスタンス間の通信は、送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたＶＮＩＣを使用して容易にされる。例えば、サブネット１内の計算インスタンスＣ１は、サブネット１内の計算インスタンスＣ２にパケットを送信したいことがある。送信元計算インスタンスから発生し、送信先が同じサブネット内の別の計算インスタンスであるパケットの場合、パケットは、送信元計算インスタンスに関連付けられたＶＮＩＣによって最初に処理される。送信元計算インスタンスに関連付けられたＶＮＩＣによって実行される処理は、パケットヘッダーからパケットの送信先情報を決定すること、送信元計算インスタンスに関連付けられたＶＮＩＣのために構成された任意のポリシー（例えば、セキュリティリスト）を識別すること、パケットのネクストホップを決定すること、必要に応じて任意のパケットカプセル化／カプセル解除機能を実行すること、およびその後、意図された送信先とのパケットの通信を容易にすることを目

的に、パケットをネクストホップに転送／ルーティングすることを含むことができる。送信先計算インスタンスが送信元計算インスタンスと同じサブネット内にある場合、送信元計算インスタンスに関連付けられたＶＮＩＣは、送信先計算インスタンスに関連付けられたＶＮＩＣを識別し、パケットを処理するためにそのＶＮＩＣに転送するように構成される。次に、送信先計算インスタンスに関連付けられたＶＮＩＣが実行され、パケットを送信先計算インスタンスに転送する。

【００５９】

サブネット内の計算インスタンスから同じＶＣＮ内の異なるサブネット内のエンドポイントに伝達されるパケットの場合、この通信は、送信元および送信先計算インスタンスに関連付けられたＶＮＩＣならびにＶＣＮ　ＶＲによって容易にされる。例えば、図１のサブネット１内の計算インスタンスＣ１が、パケットをサブネット２内の計算インスタンスＤ１に送信したい場合、このパケットは、計算インスタンスＣ１に関連付けられたＶＮＩＣによって最初に処理される。計算インスタンスＣ１に関連付けられたＶＮＩＣは、ＶＣＮ　ＶＲのデフォルトのルートまたはポート１０．０．０．１を使用してパケットをＶＣＮ　ＶＲ１０５にルーティングするように構成される。ＶＣＮ　ＶＲ１０５は、ポート１０．１．０．１を使用してパケットをサブネット２にルーティングするように構成される。次に、Ｄ１に関連付けられたＶＮＩＣによってパケットが受信されて処理され、ＶＮＩＣは、パケットを計算インスタンスＤ１に転送する。

【００６０】

ＶＣＮ１０４内の計算インスタンスからＶＣＮ１０４の外側にあるエンドポイントに伝達されるパケットのために、送信元計算インスタンスに関連付けられたＶＮＩＣ、ＶＣＮＶＲ１０５、およびＶＣＮ１０４に関連付けられたゲートウェイによって、通信が容易にされる。１つまたは複数の種類のゲートウェイが、ＶＣＮ１０４に関連付けられてよい。ゲートウェイは、ＶＣＮと別のエンドポイントの間のインターフェイスであり、別のエンドポイントはＶＣＮの外側にある。ゲートウェイは、レイヤ３／ＩＰレイヤの概念であり、ＶＣＮがＶＣＮの外側のエンドポイントと通信することを可能にする。したがって、ゲートウェイは、ＶＣＮと他のＶＣＮまたはネットワークとの間のトラフィックフローを容易にする。さまざまな種類のゲートウェイが、さまざまな種類のエンドポイントとのさまざまな種類の通信を容易にするように、ＶＣＮのために構成されてよい。ゲートウェイに応じて、通信は、パブリックネットワーク（例えば、インターネット）を経由するか、またはプライベートネットワークを経由してよい。さまざまな通信プロトコルが、これらの通信に使用されてよい。

【００６１】

例えば、計算インスタンスＣ１は、ＶＣＮ１０４の外側のエンドポイントと通信したいことがある。送信元計算インスタンスＣ１に関連付けられたＶＮＩＣによって、パケットが最初に処理されてよい。このＶＮＩＣの処理は、パケットの送信先がＣ１のサブネット１の外側にあるということを決定する。Ｃ１に関連付けられたＶＮＩＣは、パケットをＶＣＮ１０４のＶＣＮ　ＶＲ１０５に転送してよい。次にＶＣＮ　ＶＲ１０５は、パケットを処理し、この処理の一部として、パケットの送信先に基づいて、パケットのネクストホップとして、ＶＣＮ１０４に関連付けられた特定のゲートウェイを決定する。その後、ＶＣＮ　ＶＲ１０５は、パケットを特定の識別されたゲートウェイに転送してよい。例えば、送信先が顧客のオンプレミスネットワーク内のエンドポイントである場合、ＶＣＮ　ＶＲ１０５によってパケットが、ＶＣＮ１０４のために構成されたダイナミックルーティングゲートウェイ（ＤＲＧ：Dynamic Routing Gateway）ゲートウェイ１２２に転送されてよい。次に、パケットは、最終的な意図された送信先へのパケットの伝達を容易にするために、ゲートウェイからネクストホップに転送されてよい。

【００６２】

さまざまな種類のゲートウェイが、ＶＣＮのために構成されてよい。ＶＣＮのために構成され得るゲートウェイの例が、図１に示されており、下で説明される。ＶＣＮに関連付けられたゲートウェイの例は、図１８、図１９、図２０、および図２１（例えば、参照番

号１８３４、１８３６、１８３８、１９３４、１９３６、１９３８、２０３４、２０３６、２０３８、２１３４、２１３６、および２１３８によって参照されるゲートウェイ）にも示されており、下で説明される。図１に示された実施形態に示されているように、ダイナミックルーティングゲートウェイ（ＤＲＧ）１２２は、顧客のＶＣＮ１０４に追加されるか、または関連付けられてよく、顧客のＶＣＮ１０４と別のエンドポイントの間のプライベートネットワークトラフィック通信のための経路を提供し、この別のエンドポイントは、顧客のオンプレミスネットワーク１１６、ＣＳＰＩ１０１の異なるリージョン内のＶＣＮ１０８、またはＣＳＰＩ１０１によってホストされていない他のリモートクラウドネットワーク１１８であることができる。顧客のオンプレミスネットワーク１１６は、顧客のリソースを使用して構築された顧客のネットワークまたは顧客のデータセンターであってよい。顧客のオンプレミスネットワーク１１６へのアクセスは、通常、極めて制限される。顧客のオンプレミスネットワーク１１６、およびＣＳＰＩ１０１によってクラウド内でデプロイまたはホストされた１つまたは複数のＶＣＮ１０４の両方を有する顧客の場合、顧客は、顧客のオンプレミスネットワーク１１６および顧客のクラウドベースのＶＣＮ１０４が互いに通信できることを望むことがある。これによって、顧客が、ＣＳＰＩ１０１によってホストされた顧客のＶＣＮ１０４および顧客のオンプレミスネットワーク１１６を包含する拡張されたハイブリッド環境を構築することを可能にする。ＤＲＧ１２２は、この通信を可能にする。そのような通信を可能にするために、通信チャネル１２４が設定され、このチャネルの１つのエンドポイントが、顧客のオンプレミスネットワーク１１６内にあり、他のエンドポイントが、ＣＳＰＩ１０１内にあり、顧客のＶＣＮ１０４に接続される。通信チャネル１２４は、インターネットなどのパブリック通信ネットワークまたはプライベート通信ネットワークを経由することができる。インターネットなどのパブリック通信ネットワークを経由するＩＰｓｅｃ　ＶＰＮ技術、パブリックネットワークの代わりにプライベートネットワークを使用するOracleのFastConnect技術などの、さまざまな通信プロトコルが使用されてよい。通信チャネル１２４の１つのエンドポイントを形成する顧客のオンプレミスネットワーク１１６内のデバイスまたは機器は、図１に示されたＣＰＥ１２６などの、加入者宅内機器（ＣＰＥ：customer premise equipment）と呼ばれる。ＣＳＰＩ１０１側では、エンドポイントは、ＤＲＧ１２２を実行するホストマシンであってよい。

【００６３】

ある実施形態では、顧客が１つのＶＣＮを異なるリージョン内の別のＶＣＮとピアリングすることを可能にする、リモートピアリング接続（ＲＰＣ：Remote Peering Connection）がＤＲＧに追加され得る。そのようなＲＰＣを使用すると、顧客のＶＣＮ１０４は、ＤＲＧ１２２を使用して、別のリージョン内のＶＣＮ１０８と接続することができる。ＤＲＧ１２２は、Microsoft Azureクラウド、Amazon AWSクラウドなどの、ＣＳＰＩ１０１によってホストされていない他のリモートクラウドネットワーク１１８と通信するために使用されてもよい。

【００６４】

図１に示されているように、ＶＣＮ１０４上の計算インスタンスが、インターネットなどのパブリックネットワークを経由してアクセス可能なパブリックエンドポイント１１４と通信することを可能にするインターネットゲートウェイ（ＩＧＷ：Internet Gateway）１２０が、顧客のＶＣＮ１０４のために構成されてよい。ＩＧＷ１２０は、ＶＣＮをインターネットなどのパブリックネットワークに接続するゲートウェイである。ＩＧＷ１２０は、ＶＣＮ１０４などのＶＣＮ内のパブリックサブネット（パブリックサブネット内のリソースは、パブリックオーバーレイＩＰアドレスを有する）の、インターネットなどのパブリックネットワーク１１４上のパブリックエンドポイント１１２への直接アクセスを可能にする。ＩＧＷ１２０を使用して、ＶＣＮ１０４内のサブネットから、またはインターネットから、接続が開始され得る。

【００６５】

ネットワークアドレス変換（ＮＡＴ：Network Address Translation）ゲートウェ

イ１２８が、顧客のＶＣＮ１０４のために構成され、専用パブリックオーバーレイＩＰアドレスを有さない顧客のＶＣＮ内のクラウドリソースのインターネットへのアクセスを可能にし、ネットワークアドレス変換ゲートウェイ１２８は、それらのリソースを直接着信インターネット接続（例えば、Ｌ４－Ｌ７接続）に公開せずに、そのようなアクセスを可能にする。これによって、ＶＣＮ１０４内のプライベートサブネット１などの、ＶＣＮ内のプライベートサブネットの、インターネット上のパブリックエンドポイントへのプライベートアクセスを可能にする。ＮＡＴゲートウェイでは、プライベートサブネットからパブリックインターネットへの接続のみが開始されることが可能であり、インターネットからプライベートサブネットへの接続は開始され得ない。

【００６６】

ある実施形態では、サービスゲートウェイ（ＳＧＷ：Service Gateway）１２６が、顧客のＶＣＮ１０４のために構成されることが可能であり、ＶＣＮ１０４とサービスネットワーク１１０内のサポートされているサービスエンドポイントの間のプライベートネットワークトラフィックのための経路を提供する。ある実施形態では、サービスネットワーク１１０は、ＣＳＰによって提供されてよく、さまざまなサービスを提供してよい。そのようなサービスネットワークの例は、顧客によって使用され得るさまざまなサービスを提供するOracleのServices Networkである。例えば、顧客のＶＣＮ１０４のプライベートサブネット内の計算インスタンス（例えば、データベースシステム）は、パブリックＩＰアドレスもインターネットへのアクセスも必要とせずに、データをサービスエンドポイント（例えば、オブジェクトストレージ）にバックアップすることができる。ある実施形態では、ＶＣＮは、１つのみのＳＧＷを含むことができ、接続は、ＶＣＮ内のサブネットのみから開始されることが可能であり、サービスネットワーク１１０からは開始され得ない。ＶＣＮが別のＶＣＮとピアリングされた場合、通常、他のＶＣＮ内のリソースは、ＳＧＷにアクセスできない。FastConnectまたはＶＰＮ接続を使用してＶＣＮに接続されているオンプレミスネットワーク内のリソースは、そのＶＣＮのために構成されたサービスゲートウェイを使用することもできる。

【００６７】

ある実装では、ＳＧＷ１２６は、対象のサービスまたはサービスのグループのすべてのリージョンのパブリックＩＰアドレス範囲を表す文字列である、サービスクラスレスドメイン間ルーティング（ＣＩＤＲ）ラベルの概念を使用する。顧客は、サービスへのトラフィックを制御するようにＳＧＷおよび関連するルートルールを構成するときに、サービスＣＩＤＲラベルを使用する。顧客は、任意選択的に、セキュリティルールを構成するときに、サービスＣＩＤＲラベルを利用することができ、将来、サービスのパブリックＩＰアドレスが変化する場合に、それらのセキュリティルールを調整する必要がない。

【００６８】

ローカルピアリングゲートウェイ（ＬＰＧ：Local Peering Gateway）１３２は、顧客のＶＣＮ１０４に追加され得るゲートウェイであり、ＶＣＮ１０４が同じリージョン内の別のＶＣＮとピアリングすることを可能にする。ピアリングは、トラフィックがインターネットなどのパブリックネットワークを横断せず、または顧客のオンプレミスネットワーク１１６を通ってトラフィックをルーティングすることもなく、ＶＣＮが、プライベートＩＰアドレスを使用して通信することを意味する。好ましい実施形態では、ＶＣＮは、確立するピアリングごとに別々のＬＰＧを含む。ローカルピアリングまたはＶＣＮピアリングは、異なるアプリケーションまたはインフラストラクチャ管理機能間でネットワーク接続を確立するために使用される一般的な方法である。

【００６９】

サービスネットワーク１１０内のサービスのプロバイダなどのサービスプロバイダは、さまざまなアクセスモデルを使用してサービスへのアクセスを提供してよい。パブリックアクセスモデルによれば、サービスは、インターネットなどのパブリックネットワークを介して顧客のＶＣＮ内の計算インスタンスによってパブリックにアクセス可能である、およびまたはＳＧＷ１２６を介してプライベートにアクセス可能であってよい、パブリック

エンドポイントとして公開されてよい。特定のプライベートアクセスモデルによれば、サービスは、顧客のＶＣＮ内のプライベートサブネット内のプライベートＩＰエンドポイントとしてアクセス可能にされる。このアクセスは、プライベートエンドポイント（ＰＥ：Private Endpoint）アクセスと呼ばれ、サービスプロバイダがサービスを顧客のプライベートネットワーク内のインスタンスとして公開することを可能にする。プライベートエンドポイントのリソースは、顧客のＶＣＮ内のサービスを表す。各ＰＥは、顧客のＶＣＮ内の顧客によって選択されたサブネット内のＶＮＩＣ（１つまたは複数のプライベートＩＰを有するＰＥ－ＶＮＩＣと呼ばれる）として現れる。したがって、ＰＥは、ＶＮＩＣを使用して、プライベートな顧客のＶＣＮのサブネット内のサービスを提示するための方法を提供する。エンドポイントがＶＮＩＣとして公開されるため、ルーティングルール、セキュリティリストなどの、ＶＮＩＣに関連付けられたすべての特徴は、ＰＥ　ＶＮＩＣに使用可能になっている。

【００７０】

サービスプロバイダは、ＰＥを介してアクセスを可能にするために、サービスを登録することができる。プロバイダは、サービスの可視性を顧客のテナンシに制限するポリシーを、サービスに関連付けることができる。プロバイダは、特にマルチテナントサービスの場合、単一の仮想ＩＰアドレス（ＶＩＰ：virtual IP address）の下で、複数のサービスを登録することができる。同じサービスを表す（複数のＶＣＮ内の）複数のそのようなプライベートエンドポイントが存在してよい。

【００７１】

次に、プライベートサブネット内の計算インスタンスは、ＰＥ　ＶＮＩＣのプライベートＩＰアドレスまたはサービスのＤＮＳ名を使用してサービスにアクセスすることができる。顧客のＶＣＮ内の計算インスタンスは、トラフィックを顧客のＶＣＮ内のＰＥのプライベートＩＰアドレスに送信することによって、サービスにアクセスすることができる。プライベートアクセスゲートウェイ（ＰＡＧＷ：Private Access Gateway）１３０は、サービスプロバイダのＶＣＮ（例えば、サービスネットワーク１１０内のＶＣＮ）に接続され得るゲートウェイリソースであり、顧客のサブネットのプライベートエンドポイントとの間のすべてのトラフィックの入口／出口ポイントとして機能する。ＰＡＧＷ１３０は、プロバイダが内部のＩＰアドレスリソースを利用せずにＰＥの接続数をスケーリングすることを可能にする。プロバイダは、単一のＶＣＮ内で登録された任意の数のサービスに対して、１つのＰＡＧＷのみを構成する必要がある。プロバイダは、サービスを１人または複数の顧客の複数のＶＣＮ内のプライベートエンドポイントとして表すことができる。顧客の視点からは、ＰＥ　ＶＮＩＣは、顧客のインスタンスに接続される代わりに、顧客が対話することを望むサービスに接続されているように見える。プライベートエンドポイントに行くトラフィックは、ＰＡＧＷ１３０を介してサービスにルーティングされる。これらは、顧客－サービス間プライベート接続（Ｃ２Ｓ（customer-to-service）接続）と呼ばれる。

【００７２】

ＰＥの概念は、トラフィックがFastConnect/IPsecリンクおよび顧客のＶＣＮ内のプライベートエンドポイントを通って流れることを可能にすることによって、サービスのプライベートアクセスを顧客のオンプレミスネットワークおよびデータセンターに拡張するために使用されることも可能である。サービスのプライベートアクセスは、トラフィックがＬＰＧ１３２と顧客のＶＣＮ内のＰＥの間を流れることを可能にすることによって、顧客のピアリングされたＶＣＮに拡張されることも可能である。

【００７３】

顧客は、サブネットレベルでＶＣＮ内のルーティングを制御することができ、そのため顧客は、ＶＣＮ１０４などの顧客のＶＣＮ内のどのサブネットが各ゲートウェイを使用するかを指定することができる。トラフィックが特定のゲートウェイを通ってＶＣＮから外に出ることを許容されるかどうかを判定するために、ＶＣＮのルートテーブルが使用される。例えば、特定の例では、顧客のＶＣＮ１０４内のパブリックサブネットのルートテー

ブルは、ＩＧＷ１２０を介して非ローカルトラフィックを送信してよい。同じ顧客のＶＣＮ１０４内のプライベートサブネットのルートテーブルは、ＳＧＷ１２６を介してＣＳＰサービスに行くトラフィックを送信してよい。すべての残りのトラフィックは、ＮＡＴゲートウェイ１２８を介して送信されてよい。ルートテーブルは、ＶＣＮから出るトラフィックのみを制御する。

【００７４】

ＶＣＮに関連付けられたセキュリティリストは、インバウンド接続を経由してゲートウェイを介してＶＣＮに入るトラフィックを制御するために使用される。サブネット内のすべてのリソースは、同じルートテーブルおよびセキュリティリストを使用する。セキュリティリストは、ＶＣＮのサブネット内のインスタンスに入ること、およびインスタンスから出ることを許可された特定の種類のトラフィックを制御するために使用されてよい。セキュリティリストルールは、入口（インバウンド）ルールおよび出口（アウトバウンド）ルールを含んでよい。例えば、入口ルールは、許可された送信元アドレス範囲を指定してよく、一方、出口ルールは、許可された送信先アドレス範囲を指定してよい。セキュリティルールは、特定のプロトコル（例えば、ＴＣＰ、ＩＣＭＰ）、特定のポート（例えば、ＳＳＨの場合は２２、Windows RDPの場合は３３８９）などを指定してよい。ある実装では、インスタンスのオペレーティングシステムは、セキュリティリストルールと一致する、それ自体のファイアウォールルールを強制してよい。ルールは、ステートフル（例えば、接続が追跡され、応答トラフィックに関する明示的なセキュリティリストルールを使用しないで、応答が自動的に許可される）またはステートレスであってよい。

【００７５】

顧客のＶＣＮからの（すなわち、ＶＣＮ１０４にデプロイされたリソースまたは計算インスタンスによる）アクセスは、パブリックアクセス、プライベートアクセス、または専用アクセスとして分類され得る。パブリックアクセスは、パブリックエンドポイントにアクセスするためにパブリックＩＰアドレスまたはＮＡＴが使用されるアクセスモデルのことを指す。プライベートアクセスは、プライベートＩＰアドレスを有するＶＣＮ１０４内の顧客のワークロード（例えば、プライベートサブネット内のリソース）が、インターネットなどのパブリックネットワークを横断せずにサービスにアクセスすることを可能にする。ある実施形態では、ＣＳＰＩ１０１は、プライベートＩＰアドレスを有する顧客のＶＣＮのワークロードが、サービスゲートウェイを使用してサービス（のパブリックサービスエンドポイント）にアクセスすることを可能にする。したがって、サービスゲートウェイは、顧客のＶＣＮと顧客のプライベートネットワークの外側に存在するサービスのパブリックエンドポイントとの間の仮想リンクを確立することによって、プライベートアクセスモデルを提供する。

【００７６】

さらに、ＣＳＰＩは、FastConnectパブリックピアリングなどの技術を使用して専用パブリックアクセスを提供してよく、このアクセスでは、顧客のオンプレミスインスタンスが、FastConnect接続を使用して、インターネットなどのパブリックネットワークを横断せずに、顧客のＶＣＮ内の１つまたは複数のサービスにアクセスすることができる。ＣＳＰＩは、FastConnectプライベートピアリングを使用して専用プライベートアクセスを提供してもよく、このアクセスでは、プライベートＩＰアドレスを有する顧客のオンプレミスインスタンスが、FastConnect接続を使用して顧客のＶＣＮのワークロードにアクセスすることができる。FastConnectは、顧客のオンプレミスネットワークをＣＳＰＩおよびそのサービスに接続するための、パブリックインターネットを使用することに代わるネットワーク接続である。FastConnectは、インターネットに基づく接続と比較した場合に、より高い帯域幅の選択肢およびより信頼できる一貫性のあるネットワーク体験を伴う専用のプライベート接続を作成するための、容易で弾力性のある経済的な方法を提供する。

【００７７】

図１および上記の付随する説明は、例示的な仮想ネットワーク内のさまざまな仮想コン

ポーネントを説明する。前述したように、仮想ネットワークは、基盤になる物理ネットワークまたは基板ネットワークの上に構築される。図２は、ある実施形態に従って、仮想ネットワークのための基盤になるＣＳＰＩ２００内の物理ネットワークにおける物理コンポーネントの簡略化されたアーキテクチャ図を示している。図に示されているように、ＣＳＰＩ２００は、クラウドサービスプロバイダ（ＣＳＰ）によって提供されたコンポーネントおよびリソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）を含んでいる分散環境を提供する。これらのコンポーネントおよびリソースは、クラウドサービス（例えば、ＩａａＳサービス）を、加入している顧客、すなわち、ＣＳＰによって提供された１つまたは複数のサービスに加入している顧客に提供するために使用される。顧客が加入したサービスに基づいて、ＣＳＰＩ２００のリソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）のサブセットが、顧客のためにプロビジョニングされる。次に、顧客は、ＣＳＰＩ２００によって提供された物理的な計算リソース、メモリリソース、およびネットワークリソースを使用して、自分自身のクラウドベースの（すなわち、ＣＳＰＩによってホストされた）カスタマイズ可能なプライベート仮想ネットワークを構築することができる。すでに示されたように、これらの顧客のネットワークは、仮想クラウドネットワーク（ＶＣＮ）と呼ばれる。顧客は、計算インスタンスなどの１つまたは複数の顧客のリソースを、これらの顧客のＶＣＮにデプロイすることができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどの形態であることができる。ＣＳＰＩ２００は、顧客が高度に利用可能なホストされた環境内で広範囲のアプリケーションおよびサービスを構築して実行できるようにする、インフラストラクチャおよび一連の補完するクラウドサービスを提供する。

【００７８】

図２に示された実施形態例では、ＣＳＰＩ２００の物理コンポーネントは、１つまたは複数の物理ホストマシンまたは物理サーバ（例えば、２０２、２０６、２０８）、ネットワーク仮想化デバイス（ＮＶＤ）（例えば、２１０、２１２）、トップオブラック（ＴＯＲ）スイッチ（例えば、２１４、２１６）、ならびに物理ネットワーク（例えば、２１８）、および物理ネットワーク２１８内のスイッチを含む。物理ホストマシンまたは物理サーバは、ＶＣＮの１つまたは複数のサブネットに参加するさまざまな計算インスタンスをホストし、実行してよい。計算インスタンスは、仮想マシンインスタンスおよびベアメタルインスタンスを含んでよい。例えば、図１に示されたさまざまな計算インスタンスは、図２に示された物理ホストマシンによってホストされてよい。ＶＣＮ内の仮想マシン計算インスタンスは、１つのホストマシンによって、または複数の異なるホストマシンによって、実行されてよい。物理ホストマシンは、仮想ホストマシン、コンテナベースのホストまたは機能などをホストしてもよい。図１に示されたＶＮＩＣおよびＶＣＮ　ＶＲは、図２に示されたＮＶＤによって実行されてよい。図１に示されたゲートウェイは、ホストマシンによって、および／または図２に示されたＮＶＤによって、実行されてよい。

【００７９】

ホストマシンまたはサーバは、ホストマシン上の仮想環境を作成して有効化するハイパーバイザ（仮想マシンモニタまたはＶＭＭ（virtual machine monitor）とも呼ばれる）を実行してよい。仮想化環境または仮想環境は、クラウドベースのコンピューティングを容易にする。ホストマシン上で、そのホストマシン上のハイパーバイザによって、１つまたは複数の計算インスタンスが作成、実行、および管理されてよい。ホストマシン上のハイパーバイザは、ホストマシンの物理的コンピューティングリソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）が、ホストマシンによって実行されるさまざまな計算インスタンス間で共有されることを可能にする。

【００８０】

例えば、図２に示されているように、ホストマシン２０２および２０８は、ハイパーバイザ２６０および２６６をそれぞれ実行する。これらのハイパーバイザは、ソフトウェア、ファームウェア、またはハードウェア、あるいはこれらの組合せを使用して実装されてよい。通常、ハイパーバイザは、ホストマシンのオペレーティングシステム（ＯＳ：ope

rating system）の上に存在するプロセスまたはソフトウェアレイヤであり、オペレーティングシステムは、ホストマシンのハードウェアプロセッサ上で実行される。ハイパーバイザは、ホストマシンの物理的コンピューティングリソース（例えば、プロセッサ／コアなどの処理リソース、メモリリソース、ネットワークリソース）が、ホストマシンによって実行されるさまざまな仮想マシン計算インスタンス間で共有されることを可能にすることによって、仮想環境を提供する。例えば、図２では、ハイパーバイザ２６０は、ホストマシン２０２のＯＳの上に存在してよく、ホストマシン２０２のコンピューティングリソース（例えば、処理リソース、メモリリソース、およびネットワークリソース）が、ホストマシン２０２によって実行される計算インスタンス（例えば、仮想マシン）間で共有されることを可能にする。仮想マシンは、ホストマシンのＯＳと同じであるか、または異なってよい、それ自体のオペレーティングシステム（ゲストオペレーティングシステムと呼ばれる）を有することができる。ホストマシンによって実行される仮想マシンのオペレーティングシステムは、同じホストマシンによって実行される別の仮想マシンのオペレーティングシステムと同じであるか、または異なってよい。したがって、ハイパーバイザは、複数のオペレーティングシステムが、ホストマシンの同じコンピューティングリソースを共有しながら互いに並行して実行されることを可能にする。図２に示されたホストマシンは、同じ種類または異なる種類のハイパーバイザを有してよい。

【００８１】

計算インスタンスは、仮想マシンインスタンスまたはベアメタルインスタンスであることができる。図２では、ホストマシン２０２上の計算インスタンス２６８およびホストマシン２０８上の計算インスタンス２７４は、仮想マシンインスタンスの例である。ホストマシン２０６は、顧客に提供されているベアメタルインスタンスの例である。

【００８２】

ある例では、ホストマシン全体が単一の顧客にプロビジョニングされてよく、そのホストマシンによってホストされた１つまたは複数の計算インスタンス（仮想マシンまたはベアメタルインスタンスのいずれか）のすべてが、その同じ顧客に属する。他の例では、ホストマシンは、複数の顧客（すなわち、複数のテナント）間で共有されてよい。そのようなマルチテナンシの状況では、ホストマシンは、異なる顧客に属する仮想マシン計算インスタンスをホストしてよい。これらの計算インスタンスは、異なる顧客の異なるＶＣＮのメンバーであってよい。ある実施形態では、ベアメタル計算インスタンスは、ハイパーバイザを有さないベアメタルサーバによってホストされる。ベアメタル計算インスタンスがプロビジョニングされる場合、単一の顧客またはテナントが、ベアメタルインスタンスをホストしているホストマシンの物理的ＣＰＵ、メモリ、およびネットワークインターフェイスの制御を維持し、ホストマシンが、他の顧客またはテナントと共有されない。

【００８３】

前述のように、ＶＣＮの一部である各計算インスタンスは、計算インスタンスがＶＣＮのサブネットのメンバーになることを可能にするＶＮＩＣに関連付けられる。計算インスタンスに関連付けられたＶＮＩＣは、計算インスタンスとの間のパケットまたはフレームの通信を容易にする。ＶＮＩＣは、計算インスタンスが作成されるときに、計算インスタンスに関連付けられる。ある実施形態では、ホストマシンによって実行される計算インスタンスの場合、その計算インスタンスに関連付けられたＶＮＩＣが、ホストマシンに接続されたＮＶＤによって実行される。例えば、図２では、ホストマシン２０２が、ＶＮＩＣ２７６に関連付けられている仮想マシン計算インスタンス２６８を実行し、ＶＮＩＣ２７６が、ホストマシン２０２に接続されたＮＶＤ２１０によって実行される。別の例として、ホストマシン２０６によってホストされたベアメタルインスタンス２７２が、ホストマシン２０６に接続されたＮＶＤ２１２によって実行されるＶＮＩＣ２８０に関連付けられる。さらに別の例として、ＶＮＩＣ２８４が、ホストマシン２０８によって実行される計算インスタンス２７４に関連付けられ、ＶＮＩＣ２８４は、ホストマシン２０８に接続されたＮＶＤ２１２によって実行される。

【００８４】

ホストマシンによってホストされた計算インスタンスの場合、そのホストマシンに接続されたＮＶＤは、それらの計算インスタンスがメンバーであるＶＣＮに対応するＶＣＮ　ＶＲも実行する。例えば、図２に示された実施形態では、ＮＶＤ２１０は、計算インスタンス２６８がメンバーであるＶＣＮに対応するＶＣＮ　ＶＲ２７７を実行する。ＮＶＤ２１２は、ホストマシン２０６および２０８によってホストされた計算インスタンスに対応するＶＣＮに対応する１つまたは複数のＶＣＮ　ＶＲ２８３を実行してもよい。

【００８５】

ホストマシンは、ホストマシンが他のデバイスに接続されることを可能にする１つまたは複数のネットワークインターフェイスカード（ＮＩＣ）を含んでよい。ホストマシン上のＮＩＣは、ホストマシンが別のデバイスに通信可能に接続されることを可能にする１つまたは複数のポート（またはインターフェイス）を提供してよい。例えば、ホストマシンは、ホストマシンおよびＮＶＤに設けられた１つまたは複数のポート（またはインターフェイス）を使用してＮＶＤに接続されてよい。ホストマシンは、別のホストマシンなどの他のデバイスに接続されてもよい。

【００８６】

例えば、図２では、ホストマシン２０２は、ホストマシン２０２のＮＩＣ２３２によって提供されたポート２３４とＮＶＤ２１０のポート２３６の間に延びるリンク２２０を使用して、ＮＶＤ２１０に接続される。ホストマシン２０６は、ホストマシン２０６のＮＩＣ２４４によって提供されたポート２４６とＮＶＤ２１２のポート２４８の間に延びるリンク２２４を使用して、ＮＶＤ２１２に接続される。ホストマシン２０８は、ホストマシン２０８のＮＩＣ２５０によって提供されたポート２５２とＮＶＤ２１２のポート２５４の間に延びるリンク２２６を使用して、ＮＶＤ２１２に接続される。

【００８７】

次に、ＮＶＤは、物理ネットワーク２１８に接続されている（スイッチファブリックとも呼ばれる）トップオブラック（ＴＯＲ）スイッチへの通信リンクを介して接続される。ある実施形態では、ホストマシンとＮＶＤの間およびＮＶＤとＴＯＲスイッチの間のリンクは、イーサネットリンクである。例えば、図２では、リンク２２８および２３０を使用して、ＮＶＤ２１０および２１２がＴＯＲスイッチ２１４および２１６にそれぞれ接続される。ある実施形態では、リンク２２０、２２４、２２６、２２８、および２３０は、イーサネットリンクである。ＴＯＲに接続されているホストマシンおよびＮＶＤの集合は、ラックと呼ばれることがある。

【００８８】

物理ネットワーク２１８は、ＴＯＲスイッチが互いに通信できるようにする通信ファブリックを提供する。物理ネットワーク２１８は、多層ネットワークであることができる。ある実装では、物理ネットワーク２１８は、スイッチの多層Ｃｌｏｓネットワークであり、ＴＯＲスイッチ２１４および２１６は、多層のマルチノード物理スイッチングネットワーク２１８の葉レベルのノードを表す。２層ネットワーク、３層ネットワーク、４層ネットワーク、５層ネットワーク、および一般に、「ｎ」層ネットワークを含むが、これらに限定されない、さまざまなＣｌｏｓネットワーク構成が可能である。Ｃｌｏｓネットワークの例が、図５に示されており、下で説明される。

【００８９】

ホストマシンとＮＶＤの間で、１対１構成、多対１構成、１対多構成などの、さまざまな接続構成が可能である。１対１構成の実装では、各ホストマシンがそれ自体の別々のＮＶＤに接続される。例えば、図２では、ホストマシン２０２が、ホストマシン２０２のＮＩＣ２３２を介してＮＶＤ２１０に接続される。多対１構成では、複数のホストマシンが１つのＮＶＤに接続される。例えば、図２では、ホストマシン２０６および２０８が、ＮＩＣ２４４および２５０を介して同じＮＶＤ２１２にそれぞれ接続される。

【００９０】

１対多構成では、１つのホストマシンが複数のＮＶＤに接続される。図３は、ホストマシンが複数のＮＶＤに接続されるＣＳＰＩ３００内の例を示している。図３に示されてい

るように、ホストマシン３０２は、複数のポート３０６および３０８を含むネットワークインターフェイスカード（ＮＩＣ）３０４を備える。ホストマシン３００は、ポート３０６およびリンク３２０を介して第１のＮＶＤ３１０に接続され、ポート３０８およびリンク３２２を介して第２のＮＶＤ３１２に接続される。ポート３０６および３０８は、イーサネットポートであってよく、ホストマシン３０２とＮＶＤ３１０および３１２の間のリンク３２０および３２２は、イーサネットリンクであってよい。次に、ＮＶＤ３１０が第１のＴＯＲスイッチ３１４に接続され、ＮＶＤ３１２が第２のＴＯＲスイッチ３１６に接続される。ＮＶＤ３１０および３１２とＴＯＲスイッチ３１４および３１６の間のリンクは、イーサネットリンクであってよい。ＴＯＲスイッチ３１４および３１６は、多層物理ネットワーク３１８内の層０のスイッチングデバイスを表す。

【００９１】

図３に示された配置は、ＴＯＲスイッチ３１４を横断してＮＶＤ３１０を通り、ホストマシン３０２に向かう第１の経路、およびＴＯＲスイッチ３１６を横断してＮＶＤ３１２を通り、ホストマシン３０２に向かう第２の経路という、物理スイッチネットワーク３１８とホストマシン３０２の間の２つの別々の物理ネットワーク経路を提供する。別々の経路が、ホストマシン３０２の改善された可用性（高可用性と呼ばれる）をもたらす。経路（例えば、経路のうちの１つのリンクが故障する）またはデバイス（例えば、特定のＮＶＤが機能していない）のうちの１つに問題がある場合、他の経路がホストマシン３０２との間の通信に使用されてよい。

【００９２】

図３に示された構成では、ホストマシンのＮＩＣによって提供された２つの異なるポートを使用して、ホストマシンが２つの異なるＮＶＤに接続される。他の実施形態では、ホストマシンは、複数のＮＶＤへのホストマシンの接続を可能にする複数のＮＩＣを含んでよい。

【００９３】

再び図２を参照すると、ＮＶＤは、１つまたは複数のネットワークおよび／またはストレージ仮想化機能を実行する物理デバイスまたはコンポーネントである。ＮＶＤは、１つまたは複数の処理ユニット（例えば、ＣＰＵ、ネットワーク処理ユニット（ＮＰＵ：Network Processing Units）、ＦＰＧＡ、パケット処理パイプラインなど）、キャッシュを含むメモリ、およびポートを有する任意のデバイスであってよい。ＮＶＤの１つまたは複数の処理ユニットによって実行されるソフトウェア／ファームウェアによって、さまざまな仮想化機能が実行されてよい。

【００９４】

ＮＶＤは、さまざまな形態で実装されてよい。例えば、ある実施形態では、ＮＶＤは、組み込みプロセッサを内蔵するスマートＮＩＣまたはインテリジェントＮＩＣと呼ばれるインターフェイスカードとして実装される。スマートＮＩＣは、ホストマシン上のＮＩＣとは別のデバイスである。図２では、ＮＶＤ２１０および２１２は、ホストマシン２０２、ならびにホストマシン２０６および２０８にそれぞれ接続されたスマートＮＩＣとして実装されてよい。

【００９５】

しかし、スマートＮＩＣは、ＮＶＤの実装の単に１つの例である。さまざまな他の実装が可能である。例えば、一部の他の実装では、ＮＶＤまたはＮＶＤによって実行される１つまたは複数の機能は、１つまたは複数のホストマシン、１つまたは複数のＴＯＲスイッチ、およびＣＳＰＩ２００の他のコンポーネントに組み込まれるか、またはこれらによって実行されてよい。例えば、ＮＶＤはホストマシンにおいて具現化されてよく、ＮＶＤによって実行される機能がホストマシンによって実行される。別の例として、ＮＶＤはＴＯＲスイッチの一部であってよく、またはＴＯＲスイッチは、ＮＶＤによって実行される機能を実行するように構成されてよく、これによってＴＯＲスイッチは、パブリッククラウドに使用されるさまざまな複雑なパケット変換を実行できる。ＮＶＤの機能を実行するＴＯＲは、スマートＴＯＲと呼ばれることがある。ベアメタル（ＢＭ：bare metal）イン

スタンスではなく仮想マシン（ＶＭ：virtual machines）インスタンスが顧客に提供されるさらに他の実装では、ＮＶＤによって実行される機能が、ホストマシンのハイパーバイザの内部に実装されてよい。一部の他の実装では、ＮＶＤの機能の一部が、一連のホストマシン上で動作している集中型のサービスにオフロードされてよい。

【００９６】

ある実施形態では、図２に示されているようなスマートＮＩＣとして実装されるなどの場合、ＮＶＤは、ＮＶＤが１つまたは複数のホストマシンおよび１つまたは複数のＴＯＲスイッチに接続されることを可能にする複数の物理ポートを備えてよい。ＮＶＤ上のポートは、ホスト向きポート（「南ポート」とも呼ばれる）またはネットワーク向きまたはＴＯＲ向きポート（「北ポート」とも呼ばれる）として分類され得る。ＮＶＤのホスト向きポートは、ＮＶＤをホストマシンに接続するために使用されるポートである。図２のホスト向きポートの例は、ＮＶＤ２１０上のポート２３６、ならびにＮＶＤ２１２上のポート２４８および２５４を含む。ＮＶＤのネットワーク向きポートは、ＮＶＤをＴＯＲスイッチに接続するために使用されるポートである。図２のネットワーク向きポートの例は、ＮＶＤ２１０上のポート２５６およびＮＶＤ２１２上のポート２５８を含む。図２に示されているように、ＮＶＤ２１０は、ＮＶＤ２１０のポート２５６からＴＯＲスイッチ２１４に延びるリンク２２８を使用してＴＯＲスイッチ２１４に接続される。同様に、ＮＶＤ２１２は、ＮＶＤ２１２のポート２５８からＴＯＲスイッチ２１６に延びるリンク２３０を使用してＴＯＲスイッチ２１６に接続される。

【００９７】

ＮＶＤは、ホスト向きポートを介してホストマシンからパケットおよびフレーム（例えば、ホストマシンによってホストされた計算インスタンスによって生成されたパケットおよびフレーム）を受信し、必要なパケット処理を実行した後に、それらのパケットおよびフレームを、ＮＶＤのネットワーク向きポートを介してＴＯＲスイッチに転送してよい。ＮＶＤは、ＮＶＤのネットワーク向きポートを介してＴＯＲスイッチからパケットおよびフレームを受信してよく、必要なパケット処理を実行した後に、それらのパケットおよびフレームを、ＮＶＤのホスト向きポートを介してホストマシンに転送してよい。

【００９８】

ある実施形態では、複数のポート、およびＮＶＤとＴＯＲスイッチの間の関連付けられたリンクが存在してよい。これらのポートおよびリンクは、集約されて、複数のポートまたはリンクのリンクアグリゲータグループ（ＬＡＧ（link aggregator group）と呼ばれる）を形成してよい。リンクの集約は、２つのエンドポイント間（例えば、ＮＶＤとＴＯＲスイッチの間の）の複数の物理リンクが単一の論理リンクとして扱われることを可能にする。特定のＬＡＧ内のすべての物理リンクは、同じ速度で全二重モードで動作してよい。ＬＡＧは、帯域幅を増やし、２つのエンドポイント間の接続の信頼性を向上させるのに役立つ。ＬＡＧ内の物理リンクのうちの１つが故障した場合、トラフィックは、ＬＡＧ内の他の物理リンクのうちの１つに動的かつ透過的に再割り当てされる。集約された物理リンクは、個々のリンクより高い帯域幅を供給する。ＬＡＧに関連付けられた複数のポートが、単一の論理ポートとして扱われる。ＬＡＧの複数の物理リンクにわたってトラフィックがロードバランスされ得る。１つまたは複数のＬＡＧが、２つのエンドポイント間に構成されてよい。２つのエンドポイントが、ＮＶＤとＴＯＲスイッチの間、ホストマシンとＮＶＤの間などに存在してよい。

【００９９】

ＮＶＤは、ネットワーク仮想化機能を実装または実行する。これらの機能は、ＮＶＤによって実行されるソフトウェア／ファームウェアによって実行される。ネットワーク仮想化機能の例としては、パケットカプセル化およびカプセル解除機能、ＶＣＮネットワークを作成するための機能、ＶＣＮセキュリティリスト（ファイアウォール）機能などのネットワークポリシーを実施するための機能、ＶＣＮ内の計算インスタンスとの間でのパケットのルーティングおよび転送を容易にする機能などが挙げられるが、これらに限定されない。ある実施形態では、パケットの受信時に、ＮＶＤは、パケットを処理して、パケット

が転送されまたはルーティングされる方法を決定するために、パケット処理パイプラインを実行するように構成される。このパケット処理パイプラインの一部として、ＮＶＤは、ＶＣＮ内の計算インスタンスに関連付けられたＶＮＩＣを実行すること、ＶＣＮに関連付けられた仮想ルータ（ＶＲ）を実行すること、仮想ネットワーク内の転送またはルーティングを容易にするためのパケットのカプセル化およびカプセル解除、あるゲートウェイ（例えば、ローカルピアリングゲートウェイ）の実行、セキュリティリスト、ネットワークセキュリティグループの実施、ネットワークアドレス変換（ＮＡＴ）機能（例えば、ホストごとのパブリックＩＰからプライベートＩＰへの変換）、帯域幅調整機能、ならびに他の機能などの、オーバーレイネットワークに関連付けられた１つまたは複数の仮想機能を実行してよい。

【０１００】

ある実施形態では、ＮＶＤ内のパケット処理データ経路は、一連のパケット変換段で各々構成された、複数のパケットパイプラインを備えてよい。ある実装では、パケットの受信時に、パケットが構文解析され、単一のパイプラインに分類される。次に、パケットは、パケットが除去されるか、またはＮＶＤのインターフェイスを経由して送信されるまで、１段ずつ線形方式で処理される。これらの段は、既存の段を組み立てることによって新しいパイプラインが構築されることが可能になり、新しい段を作成して既存のパイプラインに挿入することによって、新しい機能が追加されることが可能になるように、基本機能的パケット処理構成要素（例えば、ヘッダーの妥当性確認、帯域幅調整の実施、新しいレイヤ２ヘッダーの挿入、Ｌ４ファイアウォールの実施、ＶＣＮカプセル化／カプセル解除など）を提供する。

【０１０１】

ＮＶＤは、ＶＣＮの制御プレーンおよびデータプレーンに対応する制御プレーン機能およびデータプレーン機能の両方を実行してよい。ＶＣＮ制御プレーンの例が、図１８、図１９、図２０、および図２１にも示されており（参照番号１８１６、１９１６、２０１６、および２１１６を参照）、下で説明される。ＶＣＮデータプレーンの例が、図１８、図１９、図２０、および図２１に示されており（参照番号１８１８、１９１８、２０１８、および２１１８を参照）、下で説明される。制御プレーン機能は、データが転送される方法を制御するネットワークを構成する（例えば、ルートおよびルートテーブルを設定する、ＶＮＩＣを構成するなどの）ために使用される機能を含む。ある実施形態では、すべてのオーバーレイと基板の間のマッピングを中心的に計算し、それらのマッピングをＮＶＤに、およびＤＲＧ、ＳＧＷ、ＩＧＷなどのさまざまなゲートウェイのような仮想ネットワークエッジデバイスに公開する、ＶＣＮ制御プレーンが提供される。同じメカニズムを使用して、ファイアウォールルールが公開されてもよい。ある実施形態では、ＮＶＤは、そのＮＶＤに関連するマッピングのみを取得する。データプレーン機能は、制御プレーンを使用する構成設定に基づくパケットの実際のルーティング／転送のための機能を含む。ＶＣＮデータプレーンは、顧客のネットワークパケットが基板ネットワークを横断する前に、それらのパケットをカプセル化することによって実施される。カプセル化／カプセル解除機能は、ＮＶＤで実施される。ある実施形態では、ＮＶＤは、ホストマシンに入るネットワークパケットおよびホストマシンから出るネットワークパケットをすべて傍受し、ネットワーク仮想化機能を実行するように構成される。

【０１０２】

上で示されたように、ＮＶＤは、ＶＮＩＣおよびＶＣＮ　ＶＲを含むさまざまな仮想化機能を実行する。ＮＶＤは、ＶＮＩＣに接続された１つまたは複数のホストマシンによってホストされた計算インスタンスに関連付けられているＶＮＩＣを実行してよい。例えば、図２に示されているように、ＮＶＤ２１０は、ＮＶＤ２１０に接続されたホストマシン２０２によってホストされた計算インスタンス２６８に関連付けられているＶＮＩＣ２７６の機能を実行する。別の例として、ＮＶＤ２１２は、ホストマシン２０６によってホストされたベアメタル計算インスタンス２７２に関連付けられているＶＮＩＣ２８０を実行し、ホストマシン２０８によってホストされた計算インスタンス２７４に関連付けられて

いるＶＮＩＣ２８４を実行する。ホストマシンは、異なる顧客に属する異なるＶＣＮに属する計算インスタンスをホストしてよく、ホストマシンに接続されたＮＶＤは、計算インスタンスに対応するＶＮＩＣを実行してよい（すなわち、ＶＮＩＣに関連する機能を実行してよい）。

【０１０３】

ＮＶＤは、計算インスタンスのＶＣＮに対応するＶＣＮ仮想ルータも実行する。例えば、図２に示された実施形態では、ＮＶＤ２１０は、計算インスタンス２６８が属するＶＣＮに対応するＶＣＮ　ＶＲ２７７を実行する。ＮＶＤ２１２は、ホストマシン２０６および２０８によってホストされた計算インスタンスが属する１つまたは複数のＶＣＮに対応する１つまたは複数のＶＣＮ　ＶＲ２８３を実行する。ある実施形態では、そのＶＣＮに対応するＶＣＮ　ＶＲは、そのＶＣＮに属する少なくとも１つの計算インスタンスをホストするホストマシンに接続されたすべてのＮＶＤによって実行される。ホストマシンが、異なるＶＣＮに属する計算インスタンスをホストする場合、そのホストマシンに接続されたＮＶＤは、それらの異なるＶＣＮに対応するＶＣＮ　ＶＲを実行してよい。

【０１０４】

ＶＮＩＣおよびＶＣＮ　ＶＲに加えて、ＮＶＤは、さまざまなソフトウェア（例えば、デーモン）を実行してよく、ＮＶＤによって実行されるさまざまなネットワーク仮想化機能を容易にする１つまたは複数のハードウェアコンポーネントを含んでよい。簡単にする目的で、これらのさまざまなコンポーネントは、図２に示された「パケット処理コンポーネント」として一緒にグループ化される。例えば、ＮＶＤ２１０はパケット処理コンポーネント２８６を備え、ＮＶＤ２１２はパケット処理コンポーネント２８８を備える。例えば、ＮＶＤのパケット処理コンポーネントは、ＮＶＤのポートおよびハードウェアインターフェイスとやりとりして、ＮＶＤによって受信されたパケットおよびＮＶＤを使用して伝達されたパケットをすべて監視し、ネットワーク情報を格納するように構成された、パケットプロセッサを含んでよい。ネットワーク情報は、例えば、ＮＶＤによって処理されるさまざまなネットワークフローを識別するネットワークフロー情報およびフローごとの情報（例えば、フローごとの統計値）を含んでよい。ある実施形態では、ネットワークフロー情報は、ＶＮＩＣごとに格納されてよい。パケットプロセッサは、パケットごとの操作を実行することに加えて、ステートフルＮＡＴおよびＬ４ファイアウォール（ＦＷ：firewall）を実施してよい。別の例として、パケット処理コンポーネントは、ＮＶＤによって格納された情報を１つまたは複数の異なる複製ターゲットストアに複製するように構成された複製エージェントを含んでよい。さらに別の例として、パケット処理コンポーネントは、ＮＶＤのロギング機能を実行するように構成されたロギングエージェントを含んでよい。パケット処理コンポーネントは、ＮＶＤの性能および健全性を監視するためのソフトウェア、および場合によっては、ＮＶＤに接続された他のコンポーネントの状態および健全性を監視するソフトウェアも、含んでもよい。

【０１０５】

図１は、ＶＣＮ、ＶＣＮ内のサブネット、サブネットにデプロイされた計算インスタンス、計算インスタンスに関連付けられたＶＮＩＣ、ＶＣＮのＶＲ、およびＶＣＮのために構成されたゲートウェイのセットを含む、例示的な仮想ネットワークまたはオーバーレイネットワークのコンポーネントを示している。図１に示されたオーバーレイコンポーネントは、図２に示された物理コンポーネントのうちの１つまたは複数によって実行またはホストされてよい。例えば、ＶＣＮ内の計算インスタンスは、図２に示された１つまたは複数のホストマシンによって実行またはホストされてよい。ホストマシンによってホストされた計算インスタンスの場合、その計算インスタンスに関連付けられたＶＮＩＣは、通常、そのホストマシンに接続されたＮＶＤによって実行される（すなわち、そのホストマシンに接続されたＮＶＤによって、ＶＮＩＣ機能が提供される）。ＶＣＮのＶＣＮ　ＶＲ機能は、そのＶＣＮの一部である計算インスタンスをホストしているか、または実行しているホストマシンに接続されているすべてのＮＶＤによって実行される。ＶＣＮに関連付けられたゲートウェイは、１つまたは複数の異なる種類のＮＶＤによって実行されてよい。

例えば、あるゲートウェイは、スマートＮＩＣによって実行されてよく、一方、他のゲートウェイは、１つまたは複数のホストマシンまたはＮＶＤの他の実装によって実行されてよい。

【０１０６】

前述したように、顧客のＶＣＮ内の計算インスタンスは、さまざまなエンドポイントと通信してよく、エンドポイントは、送信元計算インスタンスと同じサブネット内、または送信元計算インスタンスと同じＶＣＮ内の、異なるサブネット内にあることができ、あるいはエンドポイントは、送信元計算インスタンスのＶＣＮの外側にある。これらの通信は、計算インスタンスに関連付けられたＶＮＩＣ、ＶＣＮ　ＶＲ、およびＶＣＮに関連付けられたゲートウェイを使用して容易にされる。

【０１０７】

ＶＣＮ内の同じサブネット上の２つの計算インスタンス間の通信の場合、通信は、送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたＶＮＩＣを使用して容易にされる。送信元計算インスタンスおよび送信先計算インスタンスは、同じホストマシンによって、または異なるホストマシンによってホストされてよい。送信元計算インスタンスから生じるパケットは、送信元計算インスタンスをホストしているホストマシンから、そのホストマシンに接続されたＮＶＤに転送されてよい。ＮＶＤでは、パケット処理パイプラインを使用してパケットが処理され、パケット処理パイプラインは、送信元計算インスタンスに関連付けられたＶＮＩＣの実行を含むことができる。パケットの送信先エンドポイントが同じサブネット内にあるため、送信元計算インスタンスに関連付けられたＶＮＩＣの実行は、パケットが、送信先計算インスタンスに関連付けられたＶＮＩＣを実行しているＮＶＤに転送されることを引き起こし、次に、このＶＮＩＣは、パケットを処理して、送信先計算インスタンスに転送する。送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたＶＮＩＣは、同じＮＶＤ上（例えば、送信元計算インスタンスおよび送信先計算インスタンスが、両方とも同じホストマシンによってホストされる場合）、または異なるＮＶＤ上（例えば、送信元計算インスタンスおよび送信先計算インスタンスが、異なるＮＶＤに接続された異なるホストマシンによってホストされる場合）で実行されてよい。ＶＮＩＣは、ＮＶＤによって格納されたルーティングテーブル／転送テーブルを使用して、パケットのネクストホップを決定してよい。

【０１０８】

サブネット内の計算インスタンスから同じＶＣＮ内の異なるサブネット内のエンドポイントに伝達されるパケットの場合、送信元計算インスタンスから生じるパケットは、送信元計算インスタンスをホストしているホストマシンから、そのホストマシンに接続されたＮＶＤに伝達される。ＮＶＤでは、パケット処理パイプラインを使用してパケットが処理され、パケット処理パイプラインは、１つまたは複数のＶＮＩＣ、およびＶＣＮに関連付けられたＶＲの実行を含むことができる。例えば、パケット処理パイプラインの一部として、ＮＶＤは、送信元計算インスタンスに関連付けられたＶＮＩＣに対応する機能を実行するか、または呼び出す（ＶＮＩＣを実行する、とも呼ばれる）。ＶＮＩＣによって実行される機能は、パケット上のＶＬＡＮタグを調べることを含んでよい。パケットの送信先がサブネットの外側にあるため、ＶＣＮ　ＶＲ機能が次に呼び出され、ＮＶＤによって実行される。次に、ＶＣＮ　ＶＲは、パケットを、送信先計算インスタンスに関連付けられたＶＮＩＣを実行しているＮＶＤにルーティングする。次に、送信先計算インスタンスに関連付けられたＶＮＩＣがパケットを処理し、パケットを送信先計算インスタンスに転送する。送信元計算インスタンスおよび送信先計算インスタンスに関連付けられたＶＮＩＣは、同じＮＶＤ上（例えば、送信元計算インスタンスおよび送信先計算インスタンスが、両方とも同じホストマシンによってホストされる場合）、または異なるＮＶＤ上（例えば、送信元計算インスタンスおよび送信先計算インスタンスが、異なるＮＶＤに接続された異なるホストマシンによってホストされる場合）で実行されてよい。

【０１０９】

パケットの送信先が、送信元計算インスタンスのＶＣＮの外側である場合、送信元計算

インスタンスから生じるパケットは、送信元計算インスタンスをホストしているホストマシンから、そのホストマシンに接続されたＮＶＤに伝達される。ＮＶＤは、送信元計算インスタンスに関連付けられたＶＮＩＣを実行する。パケットの送信先エンドポイントがＶＣＮの外側にあるため、次にパケットは、そのＶＣＮのＶＣＮ　ＶＲによって処理される。ＮＶＤは、ＶＣＮ　ＶＲ機能を呼び出し、パケットが、ＶＣＮに関連付けられた適切なゲートウェイを実行しているＮＶＤに転送されることを引き起こしてよい。例えば、送信先が顧客のオンプレミスネットワーク内のエンドポイントである場合、パケットは、ＶＣＮ　ＶＲによって、ＶＣＮのために構成されたＤＲＧゲートウェイを実行しているＮＶＤに転送されてよい。ＶＣＮ　ＶＲは、送信元計算インスタンスに関連付けられたＶＮＩＣを実行しているＮＶＤと同じＮＶＤ上で、または異なるＮＶＤによって、実行されてよい。ゲートウェイは、スマートＮＩＣ、ホストマシン、または他のＮＶＤの実装であることができるＮＶＤによって、実行されてよい。次に、パケットは、ゲートウェイによって処理され、意図された送信先エンドポイントへのパケットの伝達を容易にするネクストホップに転送される。例えば、図２に示された実施形態では、計算インスタンス２６８から生じるパケットは、リンク２２０を経由して（ＮＩＣ２３２を使用して）ホストマシン２０２からＮＶＤ２１０に伝達されてよい。ＮＶＤ２１０で、ＶＮＩＣ２７６が、送信元計算インスタンス２６８に関連付けられたＶＮＩＣであるため、呼び出される。ＶＮＩＣ２７６は、パケット内のカプセル化された情報を調べ、意図された送信先エンドポイントへのパケットの伝達を容易にすることを目的に、パケットを転送するためのネクストホップを決定し、その後、パケットを決定されたネクストホップに転送するように構成される。

【０１１０】

ＶＣＮにデプロイされた計算インスタンスは、さまざまなエンドポイントと通信することができる。これらのエンドポイントは、ＣＳＰＩ２００によってホストされているエンドポイント、およびＣＳＰＩ２００の外側のエンドポイントを含んでよい。ＣＳＰＩ２００によってホストされたエンドポイントは、同じＶＣＮまたは他のＶＣＮ内のインスタンスを含んでよく、これらのＶＣＮは、顧客のＶＣＮまたは顧客に属していないＶＣＮであってよい。ＣＳＰＩ２００によってホストされたエンドポイント間の通信は、物理ネットワーク２１８を経由して実行されてよい。計算インスタンスは、ＣＳＰＩ２００によってホストされていないか、またはＣＳＰＩ２００の外側にある、エンドポイントと通信してもよい。これらのエンドポイントの例としては、顧客のオンプレミスネットワークまたはデータセンター内のエンドポイント、あるいはインターネットなどのパブリックネットワークを経由してアクセスできるパブリックエンドポイントが挙げられる。ＣＳＰＩ２００の外側のエンドポイントとの通信は、さまざまな通信プロトコルを使用して、パブリックネットワーク（例えば、インターネット）（図２に示されていない）またはプライベートネットワーク（図２に示されていない）を経由して実行されてよい。

【０１１１】

図２に示されたＣＳＰＩ２００のアーキテクチャは、単に例であり、限定することを意図されていない。代替の実施形態では、変形、代替手段、および変更が可能である。例えば、一部の実装では、ＣＳＰＩ２００は、図２に示されたシステムまたはコンポーネントより多いか、または少ないシステムまたはコンポーネントを含んでよく、２つ以上のシステムを組み合わせてよく、またはシステムの異なる構成もしくは配置を含んでよい。図２に示されたシステム、サブシステム、および他のコンポーネントは、それぞれのシステムの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）において、ハードウェアを使用して、またはこれらの組合せで実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。

【０１１２】

図４は、ある実施形態による、マルチテナンシ機能をサポートするためのＩ／Ｏ仮想化を実現するための、ホストマシンとＮＶＤの間の接続を示している。図４に示されているように、ホストマシン４０２は、仮想環境を提供するハイパーバイザ４０４を実行する。

ホストマシン４０２は、顧客／テナント１番に属するＶＭ１　４０６および顧客／テナント２番に属するＶＭ２　４０８という２つの仮想マシンインスタンスを実行する。ホストマシン４０２は、リンク４１４を介してＮＶＤ４１２に接続されている物理ＮＩＣ４１０を備える。計算インスタンスの各々は、ＮＶＤ４１２によって実行されるＶＮＩＣに接続される。図４の実施形態では、ＶＭ１　４０６はＶＮＩＣ－ＶＭ１　４２０に接続され、ＶＭ２　４０８はＶＮＩＣ－ＶＭ２　４２２に接続される。

【０１１３】

図４に示されているように、ＮＩＣ４１０は、論理ＮＩＣ　Ａ　４１６および論理ＮＩＣ　Ｂ　４１８という２つの論理ＮＩＣを備えている。各仮想マシンは、それ自体の論理ＮＩＣに接続され、その論理ＮＩＣと共に機能するように構成される。例えば、ＶＭ１　４０６は論理ＮＩＣ　Ａ　４１６に接続され、ＶＭ２　４０８は論理ＮＩＣ　Ｂ　４１８に接続される。ホストマシン４０２が、複数のテナントによって共有されている１つのみの物理ＮＩＣ４１０を備えているとしても、論理ＮＩＣに起因して、各テナントの仮想マシンは、自分のホストマシンおよびＮＩＣを有しているということを確信している。

【０１１４】

ある実施形態では、各論理ＮＩＣがそれ自体のＶＬＡＮ　ＩＤを割り当てられる。したがって、特定のＶＬＡＮ　ＩＤが、テナント１番の論理ＮＩＣ　Ａ　４１６に割り当てられ、別のＶＬＡＮ　ＩＤが、テナント２番の論理ＮＩＣ　Ｂ　４１８に割り当てられる。パケットがＶＭ１　４０６から伝達されるときに、テナント１番に割り当てられたタグが、ハイパーバイザによってパケットに取り付けられ、次に、パケットが、リンク４１４を経由してホストマシン４０２からＮＶＤ４１２に伝達される。同様の方法で、パケットがＶＭ２　４０８から伝達されるときに、テナント２番に割り当てられたタグが、ハイパーバイザによってパケットに取り付けられ、次に、パケットが、リンク４１４を経由してホストマシン４０２からＮＶＤ４１２に伝達される。したがって、ホストマシン４０２からＮＶＤ４１２に伝達されたパケット４２４は、特定のテナントおよび関連付けられたＶＭを識別する関連付けられたタグ４２６を有する。ＮＶＤで、ホストマシン４０２から受信されたパケット４２４に関して、パケットに関連付けられたタグ４２６が、パケットがＶＮＩＣ－ＶＭ１　４２０によって処理されるべきか、またはＶＮＩＣ－ＶＭ２　４２２によって処理されるべきかを判定するために使用される。次に、パケットは、対応するＶＮＩＣによって処理される。図４に示された構成は、各テナントの計算インスタンスが、自分のホストマシンおよびＮＩＣを所有しているということを確信できるようにする。図４に示された設定は、マルチテナンシ機能をサポートするためのＩ／Ｏ仮想化を可能にする。

【０１１５】

図５は、ある実施形態による、物理ネットワーク５００の簡略化されたブロック図を示している。図５に示された実施形態は、Ｃｌｏｓネットワークとして構造化される。Ｃｌｏｓネットワークは、高い２分割帯域幅および最大のリソース利用を維持しながら、接続冗長性をもたらすように設計された特定の種類ネットワークトポロジーである。Ｃｌｏｓネットワークは、ノンブロッキングの多段または多層スイッチングネットワークの一種であり、その段または層の数は、２つ、３つ、４つ、５つなどであることができる。図５に示された実施形態は、層１、２、および３を含んでいる３層ネットワークである。ＴＯＲスイッチ５０４は、Ｃｌｏｓネットワーク内の層０スイッチを表す。１つまたは複数のＮＶＤがＴＯＲスイッチに接続される。層０スイッチは、物理ネットワークのエッジデバイスとも呼ばれる。層０スイッチは、リーフスイッチとも呼ばれる層１スイッチに接続される。図５に示された実施形態では、「ｎ」個の層０ＴＯＲスイッチのセットが、「ｎ」個の層１スイッチのセットに接続され、一緒にポッドを形成する。ポッド内の各層０スイッチは、ポッド内のすべての層１スイッチに相互接続されるが、ポッド間にスイッチの接続は存在しない。ある実装では、２つのポッドはブロックと呼ばれる。各ブロックは、「ｎ」個の層２スイッチ（スパインスイッチと呼ばれることがある）のセットによってサービスを提供されるか、またはそれらに接続される。物理ネットワークトポロジーには、複数

のブロックが存在することができる。次に、層２スイッチは、「ｎ」個の層３スイッチ（スーパースパインスイッチと呼ばれることがある）に接続される。物理ネットワーク５００を経由するパケットの通信は、通常、１つまたは複数のレイヤ３通信プロトコルを使用して実行される。通常、ＴＯＲレイヤを除く物理ネットワークのすべてのレイヤは、ｎ方向の冗長性を有し、したがって、高可用性を可能にする。物理ネットワークのスケーリングを可能にするように、物理ネットワーク内で互いのスイッチの可視性を制御するために、ポッドおよびブロックに対してポリシーが指定されてよい。

【０１１６】

Ｃｌｏｓネットワークの特徴は、１つの層０スイッチから別の層０スイッチに（または層０スイッチに接続されたＮＶＤから層０スイッチに接続された別のＮＶＤに）達するための最大ホップ数が固定されることである。例えば、３層Ｃｌｏｓネットワークでは、パケットが１つのＮＶＤから別のＮＶＤに達するために、最大で７ホップが必要とされ、送信元ＮＶＤおよびターゲットＮＶＤが、Ｃｌｏｓネットワークのリーフ層に接続される。同様に、４層Ｃｌｏｓネットワークでは、パケットが１つのＮＶＤから別のＮＶＤに達するために、最大で９ホップが必要とされ、送信元ＮＶＤおよびターゲットＮＶＤが、Ｃｌｏｓネットワークのリーフ層に接続される。したがって、Ｃｌｏｓネットワークアーキテクチャは、ネットワーク全体を通じて一貫性のある待ち時間を維持し、これは、データセンター内およびデータセンター間の通信にとって重要である。Ｃｌｏｓトポロジーは、水平にスケーリングし、コスト効率が高い。より多くのスイッチ（例えば、より多くのリーフスイッチおよびスパインスイッチ）をさまざまな層に追加することによって、および隣接する層でスイッチ間のリンクの数を増やすことによって、ネットワークの帯域幅／スループット能力が容易に増やされ得る。

【０１１７】

ある実施形態では、ＣＳＰＩ内の各リソースに、クラウド識別子（ＣＩＤ：Cloud Identifier）と呼ばれる一意の識別子が割り当てられる。この識別子は、リソースの情報の一部として含まれ、例えばコンソールを介して、またはＡＰＩを介して、リソースを管理するために使用され得る。ＣＩＤの例示的な構文は次のとおりである。

ｏｃｉｄ１．＜リソースの種類＞．＜レルム＞．［リージョン］［．将来の使用］．＜一意のＩＤ＞

ここで、

ｏｃｉｄ１：ＣＩＤのバージョンを示すリテラル列。

リソースの種類：リソースの種類（例えば、インスタンス、ボリューム、ＶＣＮ、サブネット、ユーザ、グループなど）。

レルム：リソースが存在するレルム。例示的な値は、商用レルムの場合の「ｃ１」、政府クラウドレルムの場合の「ｃ２」、または連邦政府クラウドレルムの場合の「ｃ３」などである。各レルムは、それ自体のドメイン名を有してよい。

リージョン：リソースが存在するリージョン。リージョンをリソースに適用できない場合、この部分は空白であってよい。

将来の使用：将来の使用のために予約されている。

一意のＩＤ：ＩＤの一意の部分。この形式は、リソースまたはサービスの種類に応じて変わってよい。

【０１１８】

マルチクラウドの導入

図６は、ある実施形態による、異なるクラウドサービスプロバイダ（ＣＳＰ）によって提供された複数のクラウド環境を含んでいる分散環境６００の簡略化された高レベルの図を示し、クラウド環境が、その特定のクラウド環境によって提供された１つまたは複数のクラウドサービスが他のクラウド環境の顧客によって使用されることを可能にする特殊なインフラストラクチャを提供する特定のクラウド環境を含む。図６に示されているように、さまざまなクラウド環境（「クラウド」とも呼ばれる）が、異なるクラウドサービスプロバイダ（ＣＳＰ）によって提供されてよく、各クラウド環境またはクラウドは、そのク

ラウド環境の１人または複数の顧客が加入することができる１つまたは複数のクラウドサービスを提供する。ＣＳＰによって提供されたクラウド環境によって提供される一連のクラウドサービスは、ＳａａＳ（Software-as-a-Service）サービス、ＩａａＳ（Infrastructure-as-a-Service）サービス、ＰａａＳ（Platform-as-a-Service）サービス、ＤＢａａＳ（Database-as-a-Service）などを含むが、これらに限定されない、１つまたは複数の異なる種類のクラウドサービスを含んでよい。さまざまなＣＳＰによって提供されたクラウド環境の例としては、Oracle Corporationによって提供されたOracle（登録商標）クラウドインフラストラクチャ（ＯＣＩ）、Microsoft Corporationによって提供されたMicrosoft（登録商標）Azure、Google LLCによって提供されたGoogle Cloud（商標）、Amazon Corporationによって提供されたAmazon Web Services（ＡＷＳ（登録商標））などが挙げられる。特定のクラウド環境によって提供されたクラウドサービスは、別のクラウド環境によって提供されたクラウドサービスのセットと異なってよい。

【０１１９】

標準的なクラウド環境では、ＣＳＰは、そのクラウド環境によって顧客に提供されている１つまたは複数のクラウドサービスを提供するために使用されるクラウドサービスプロバイダインフラストラクチャ（ＣＳＰＩ）を提供する。ＣＳＰによって提供されたＣＳＰＩは、計算リソース、メモリリソース、ネットワークリソース、クラウドサービスにアクセスするためのコンソールなどを含む、さまざまな種類のハードウェアリソースおよびソフトウェアリソースを含んでよい。ＣＳＰによって提供されたクラウド環境の顧客は、そのクラウド環境によって提供されたクラウドサービスのうちの１つまたは複数に加入してよい。ＣＳＰによって、さまざまなサブスクリプションモデルが顧客に提供されてよい。顧客がクラウド環境によって提供されたクラウドサービスに加入した後に、１人または複数のユーザが、加入している顧客に関連付けられてよく、これらのユーザは、顧客が加入したクラウドサービスを使用することができる。ある実装では、顧客が、特定のクラウド環境によって提供されたクラウドサービスに加入するときに、顧客のアカウントまたは顧客のテナンシが、その顧客のために作成される。次に、１人または複数のユーザが、顧客のテナンシに関連付けられることが可能であり、その後、これらのユーザは、顧客のテナンシの下で顧客が加入したサービスを使用することができる。顧客が加入したサービス、顧客のテナンシに関連付けられたユーザなどに関する情報が、通常は、クラウド環境内に格納され、顧客のテナンシに関連付けられる。

【０１２０】

例えば、３つの異なるＣＳＰによって提供された３つの異なるクラウド環境が、図６に示されている。これらのクラウド環境は、ＣＳＰ　Ａによって提供されたクラウド環境Ａ（クラウドＡ）６１０、ＣＳＰ　Ｂによって提供されたクラウド環境Ｂ（クラウドＢ）６４０、およびＣＳＰ　Ｃによって提供されたクラウド環境Ｃ（クラウドＣ）６６０を含む。クラウドＡ　６１０は、ＣＳＰ　Ａによって提供されたインフラストラクチャＣＳＰＩ＿Ａ　６１２を含み、このインフラストラクチャは、クラウドＡ　６１０によって提供されたサービスのセット「サービスＡ」６１４を提供するために使用されてよい。１人または複数の顧客（例えば、顧客Ａ１　６１６－１、顧客Ａ２　６１６－２）は、クラウドＡ　６１０によって提供されたサービスＡ　６１４からの１つまたは複数のサービスに加入してよい。１人または複数のユーザ６１８－１は、顧客Ａ１　６１６－１に関連付けられてよく、クラウドＡ　６１０内で顧客Ａ１　６１６－１が加入したサービスを使用することができる。同様の方法で、１人または複数のユーザ６１８－２は、顧客Ａ２　６１６－２に関連付けられてよく、クラウドＡ　６１０内で顧客Ａ２　６１６－２が加入したサービスを使用することができる。さまざまな使用事例では、顧客Ａ１　６１６－１が加入したサービスは、顧客Ａ２　６１６－２が加入したサービスと異なってよい。

【０１２１】

図６に示されているように、クラウドＢ　６４０は、ＣＳＰ　Ｂによって提供されたインフラストラクチャＣＳＰＩ＿Ｂ　６４２を含み、このインフラストラクチャは、クラウ

ドＢ　６４０によって提供されたサービスのセット「サービスＢ」６４４を提供するために使用されてよい。１人または複数の顧客（例えば、顧客Ｂ１　６４６－１）は、サービスＢ　６４４からの１つまたは複数のサービスに加入してよい。１人または複数のユーザ６４８－１は、顧客Ｂ１　６４６－１に関連付けられてよく、クラウドＢ　６４０内で顧客Ｂ１　６４６－１が加入したサービスを使用することができる。

【０１２２】

図６に示されているように、クラウドＣ　６６０は、ＣＳＰ　Ｃによって提供されたインフラストラクチャＣＳＰＩ＿Ｃ　６６２を含み、このインフラストラクチャは、クラウドＣ　６６０によって提供されたサービスのセット「サービスＣ」６６４を提供するために使用されてよい。１人または複数の顧客（例えば、顧客Ｃ１　６６６－１）は、サービスＣ　６６４からの１つまたは複数のサービスに加入してよい。１人または複数のユーザ６６８－１は、顧客Ｃ１　６６６－１に関連付けられてよく、クラウドＣ　６６０内で顧客Ｃ１　６６６－１が加入したサービスを使用することができる。サービスＡ　６１４、サービスＢ　６４４、およびサービスＣ　６６４が互いに異なることができるということに、注意するべきである。

【０１２３】

既存のクラウドの実装では、各クラウドは、閉じたエコシステムを加入している顧客および関連付けられたユーザに提供する。その結果、クラウド環境の顧客および関連付けられたユーザは、顧客が加入しているクラウドによって提供されたサービスを使用することに制限される。例えば、顧客Ｂ１　６４６－１およびそのユーザ６４８－１は、クラウドＢ　６４０によって提供されたサービスＢ　６４４を使用することに制限され、クラウドＢ　６４０内の自分のアカウントを使用して、クラウドＡ　６１０によって提供されたサービスＡ　６１４からのサービスまたはクラウドＣ　６６０によって提供されたサービスＣ　６６４からのサービスなどの、異なるクラウド環境からのサービスにアクセスすることができない。本明細書に記載された教示は、この制限を克服する。本開示において説明されているように、リンクが２つのクラウド環境間に作成されることを可能にし、それによって、第１のＣＳＰによって提供された第１のクラウド環境によって提供されたサービスが、第２の異なるＣＳＰによって提供された第２の異なるクラウド環境の顧客（および関連付けられたユーザ）によって、第２のクラウド環境内の顧客のアカウントを使用して、使用されることを可能にする、さまざまな技術が説明される。

【０１２４】

例えば、図６に示された実施形態では、ＣＳＰ　Ａによって提供されたインフラストラクチャＣＳＰＩ＿Ａ　６１２は、他のインフラストラクチャ６２０に加えて、クラウドＡによって提供された１つまたは複数のサービス６１４が、クラウドＢ　６４０およびＣ　６６０などの他のクラウドの顧客および関連付けられたユーザによって、それらの他のクラウド内の顧客のアカウントを使用して、使用されることを可能にする、特殊なインフラストラクチャ６２２（マルチクラウド有効化インフラストラクチャ６２２またはＭＥＩ（multi-cloud enabling infrastructure）６２２あるいはマルチクラウドインフラストラクチャ６２２と呼ばれる）を含む。ある実装では、クラウドＢおよびＣの顧客は、クラウドＡ　６１０によって提供されたサービス６１４のうちの１つまたは複数を使用するために、クラウドＡを使用して別々のアカウントを開く必要がない。クラウドＢ　６４０の顧客Ｂ１　６４６－１および関連付けられたユーザ６４８－１は、クラウドＢ　６４０内の顧客のアカウントまたはテナンシを使用して、クラウドＡ　６１０によって提供された１つまたは複数のサービス６１４を使用することができる。別の例として、クラウドＣ　６６０の顧客Ｃ１　６６６－１および関連付けられたユーザ６６８－１は、クラウドＣ　６６０内の顧客のアカウントまたはテナンシを使用して、クラウドＡ　６１０によって提供された１つまたは複数のサービス６１４を使用することができる。

【０１２５】

ある実装では、ＭＥＩ６２２は、クラウドＡ　６１０と他のクラウドの間にリンクが作成されることを可能にし、これらのリンクは、クラウドＡ　６１０によって提供されたサ

ービスにアクセスして利用するために、他のクラウドの顧客および関連付けられたユーザによって使用され得る。これが、クラウドＡ　６１０とクラウドＢ　６４０の間に作成されたリンク６７０、およびクラウドＡ　６１０とクラウドＣ　６６０の間に作成されたリンク６７２として、図６に記号的に示されている。リンク６７０を介して、クラウドＢ　６４０の顧客は、クラウドＡ　６１０によって提供された１つまたは複数のサービス６１４にアクセスするか、またはサービス６１４を使用することができる。同様に、リンク６７２を介して、クラウドＣ　６６０の顧客は、クラウドＡ　６１０によって提供された１つまたは複数のサービス６１４にアクセスするか、またはサービス６１４を使用することができる。

【０１２６】

ＭＥＩ６１２が実装され得るさまざまな方法が存在する。ある実施形態では、ＭＥＩ６１２は、異なるクラウドとのリンクが確立されることを可能にするコンポーネントを含んでよい。例えば、図６では、ＭＥＩ６２２は、クラウドＢ　６４０とのリンク６７０を有効化する役割を担うインフラストラクチャコンポーネント６２４、およびクラウドＣ　６６０とのリンク６７２を有効化する役割を担うインフラストラクチャコンポーネント６２６を含む。同様の方法で、ＭＥＩ６２２は、他のクラウドとのリンクを有効化し、容易にする他のコンポーネントを含んでよい。一部の実装では、ＭＥＩ６２２のコンポーネントは、複数の異なるクラウドとのリンクを容易にしてもよい。

【０１２７】

１つのクラウドの顧客が、異なるクラウドによって提供されたクラウドサービスを使用したい理由、または使用することを望む理由は、複数ある。例として図６を使用すると、クラウドＢ　６４０の顧客Ｂ１　６４６－１がクラウドＡ　６１０によって提供されたクラウドサービス６１４を使用したい理由が複数ある。１つの使用事例の状況では、この理由は、クラウドＡ　６１０が、クラウドＢ　６４０によって提供されない機能を有するクラウドサービスを提供するために発生することがある。別の使用事例の状況として、クラウドＡおよびＢは、同様のサービスを提供することができるが、クラウドＡ　６１０によって提供されたサービスが、クラウドＢ　６４０によって提供された対応するサービスより良い（例えば、より多くの特徴／機能、より高速など）ことがある。さらに別の使用事例の状況として、クラウドＢ　６４０の顧客Ｂ１　６４６－１は、クラウドＢ　６４０によって提供されたクラウドサービスより低価格でサービスが提供されるため、クラウドＡ　６１０によって提供されたクラウドサービスを使用したいことがある。場合によっては、クラウドＢ　６４０の顧客Ｂ１　６４６－１がクラウドＡ　６１０によって提供されたクラウドサービスを使用したい、地理的制約または他の理由が存在することがある。例えば、クラウドＡ　６１０は、クラウドＢ　６４０によってサービス提供されていない所望のサービスを地理的領域内で提供することがあり、または特定のサービスが、顧客がサービスを望んでいる地理的領域内で、クラウドＢ　６４０によって提供されていない。１つのクラウドの顧客が異なるクラウドによって提供されたサービスを使用したい理由に関して、複数の他の使用事例の状況も可能である。

【０１２８】

ある実施形態では、ＭＥＩ６２２は、クラウドＡ　６１０と別のクラウドの間のリンクを作成し、このリンクを介して、他のクラウドの顧客に関連付けられたユーザが、シームレスな方法で、他のクラウド自体から、クラウドＡ　６１０によって提供されたサービスにアクセスして使用できるようにするための能力を提供し、その機能を実行する。例えば、ＭＥＩ６２２は、クラウド６４０の顧客Ｂ１　６４６－１に関連付けられたユーザ６４８－１が、シームレスな方法で、クラウドＡ　６１０によって提供されたサービスＡ　６１４からのサービスにアクセスできるようにする。ある実装では、クラウドＢ　６４０内からユーザ６４８－１がアクセスできるユーザインターフェイス（例えば、コンソール）が提供されてよく、このユーザインターフェイスは、ユーザが、クラウドＡ　６１０によって提供されたサービス６１４のリストを見ること、およびユーザ６４８－１がアクセスすることを望む特定のサービスを選択することを可能にする。ユーザの選択に応答して、

ＭＥＩ６２２は、要求されたサービスへのアクセスを可能にするために、クラウドＡとＢの間のリンク６７０を確立する処理を実行する役割を担う。リンク６７０を設定するための処理が、ＭＥＩ６２２によって実質的に自動的に実行される。顧客Ｂ１　６４６－１または関連付けられたユーザ６４８－１は、クラウドＡ　６１０とＢ　６４０の間のリンク６７０の作成、維持、および使用を容易にするために必要とされるすべてのシステム、ネットワーク、または他の構成の変更を実行することに関して、心配することがない。クラウド間のリンクの作成において、ユーザにも顧客にも負担を与えない。本開示で説明された技術を使用して、高速で効率的な方法でリンクが作成される。

【０１２９】

ＭＥＩ６２２は、さまざまな技術を使用して、ユーザおよび顧客にとってシームレスなリンクの作成および使用を行い、このようにして、改善されたユーザ体験を提供することができる。ある実装では、ＭＥＩ６２２は、クラウドＡ　６１０にサービスを要求する、およびクラウドＡ　６１０からの要求されたサービスにアクセスするなどのために、顧客Ｂ１および関連付けられたユーザ６４８－１が対話するユーザインターフェイス（例えば、グラフィカルユーザインターフェイスＧＵＩ（graphical user interfaces）など）およびプロセスフローを、クラウドＢ　６４０内で顧客／ユーザが体験するインターフェイスおよびプロセスフローに実質的に類似させる。このようにして、クラウドＢ　６４０のインターフェイスおよびプロセスフローに慣れていることがある顧客またはユーザは、クラウドＡ　６１０からのサービス６１４にアクセスするために、新しいインターフェイスおよびプロセスフローを学習する必要がない。ＭＥＩ６２２は、異なるクラウド環境のユーザに、異なるインターフェイスおよびプロセスフローを提示してよい。例えば、クラウドＢのユーザインターフェイスおよびフローに実質的に類似しているユーザインターフェイスおよびプロセスフローの第１のセットが、クラウドＢ　６４０からのユーザに提示されてよく、一方、クラウドＣのユーザインターフェイスおよびフローに実質的に類似しているユーザインターフェイスおよびプロセスフローの異なるセットが、クラウドＣ　６６０からからクラウドＡ　６１０にアクセスしているユーザに提示されてよい。これは、他のクラウドからクラウドＡ　６１０のサービス６１４にアクセスするためのユーザの体験を簡略化し、その結果、改善するために実行される。

【０１３０】

別の例として、各クラウド環境は、通常、セキュリティをクラウド環境に提供するように構成されたアイデンティティ管理システムを含む。アイデンティティ管理システムは、クラウド環境にデプロイされている、ＣＳＰによって提供されたリソース、および加入しているクラウドの顧客のリソースを含む、クラウド環境内のリソースを保護するように構成される。アイデンティティ管理システムによって実行される機能は、例えば、クラウドの加入している顧客および関連付けられたユーザに関連付けられたアイデンティティ認証情報（例えば、ユーザ名、パスワードなど）を管理すること、アイデンティティ認証情報を使用して、クラウド環境のために構成された許可／アクセスポリシーに基づいてクラウドリソースおよびサービスへのユーザのアクセスを規制すること、ならびに他の機能を含む。異なるクラウドは、異なるアイデンティティ管理システムおよび関連する技術を使用してよい。例えば、クラウドＡ　６１０内のアイデンティティ管理システムおよび関連する手順は、クラウドＢ　６４０内のアイデンティティ管理システムおよび関連する手順と完全に異なってよく、さらに、クラウドＢ　６４０内のアイデンティティ管理システムおよび関連する手順は、クラウドＣ　６６０内のアイデンティティ管理システムおよび関連する手順と完全に異なってよい。ある実装では、異なるクラウド環境間のアイデンティティ管理システムおよび関連する手順におけるこれらの違いにもかかわらず、本明細書に記載された技術は、第１のクラウドの顧客に関連付けられたユーザが、第１のクラウド内の顧客およびユーザに関連付けられた同じアイデンティティ認証情報を使用して、異なるクラウドによって提供されたクラウドサービスにアクセスすることを可能にする。

【０１３１】

例えば、図６に示された実施形態では、ＣＳＰ　Ｂによって提供されたクラウドＢ　６

４０は、アイデンティティ認証情報を、顧客Ｂ１　６４６－１および関連付けられたユーザ６４８－１などの加入している顧客および関連付けられたユーザに割り当てる（assigns）か、または割り当てる（allocates）、アイデンティティ管理システムを含んでよい。これらのアイデンティティ認証情報は、クラウドＢ　６４０内の顧客Ｂ１　６４６－１のために作成されたテナンシに関連付けられる。ある実装では、クラウドＡ　６１０によって提供されたＭＥＩ６２２は、クラウドＢの顧客Ｂ１　６４６－１に関連付けられたユーザ６４８－１が、クラウドＢ　６４０内のユーザ６４８－１および顧客Ｂ１　６４６－１に関連付けられたアイデンティティ認証情報を使用してクラウドＡ　６１０内のサービスＡ　６１４からのサービスにアクセスすることを可能にする。これによって、単にクラウドＡ　６１０内のサービス６１４にアクセスする目的で、ユーザ６４８－１がクラウドＡ　６１０に固有の新しいアイデンティティ認証情報を作成する必要がないため、ユーザ６４８－１のユーザ体験を大幅に改善する。ＭＥＩ６２２は、そのようなアクセスを容易にする。

【０１３２】

例として、クラウドＢ　６４０の顧客Ｂ１は、クラウドＡ　６１０によって提供されたサービスのセット６１４からのＤＢａａＳ（Database-as-a Service）などのサービスを使用することを選択してよい。そのような選択に応答して、ＭＥＩ６２２は、顧客Ｂ１　６４６－１に関連付けられたユーザ６４８－１がクラウドＡ　６１０によって提供されたＤＢａａＳサービスを使用できるようにするために、リンク６７０がクラウドＡ　６１０とクラウドＢ　６４０の間に自動的に作成されることを引き起こす。リンク６７０の自動的な設定は、ＭＥＩ６２２によって容易にされる。リンク６７０が設定された後に、ユーザ６４８－１は、クラウドＢ　６４０を介してクラウドＡ　６１０内のＤＢａａＳサービスを使用することができる。このサービスを使用することの一部として、ユーザ６４８－１は、クラウドＢ　６４０を介して、データベースリソースを作成する要求をクラウドＡ　６１０に送信することができる。それに応じて、ＣＳＰＩ＿Ａ　６１２は、要求されたデータベースをクラウドＡ　６１０内に作成してよい。ある実装では、作成されたデータベースは、クラウドＡ　６１０内で顧客Ｂ１のために作成された仮想ネットワーク（例えば、仮想クラウドネットワークまたはＶＣＮ）内でプロビジョニングされてよく、クラウドＢ　６４０を介してユーザ６４８－１によってアクセス可能である。次に、ユーザ６４８－１は、クラウドＢ　６４０から、プロビジョニングされたデータベースを使用する要求をクラウドＡ　６１０に送信してよい。これらの要求は、例えば、データをデータベースに書き込むこと、データベースに格納されたデータを更新すること、データベース内のデータを削除すること、データベースを削除すること、追加のデータベースを作成することなどの要求を含んでよい。一部の使用事例では、これらの要求は、クラウドＢ　６４０を介してユーザ６４８－１から、またはクラウドＢ　６４０によって提供されたサービス６４４から、生じてよい。このようにして、クラウドＡ　６１０によって提供されたＭＥＩ６２２は、異なるＣＳＰによって提供された異なるクラウドの顧客に関連付けられたユーザが、クラウドＡ　６１０によって提供されたサービスにシームレスにアクセスできるようにする。

【０１３３】

図６に示された分散環境６００は、単に例であり、主張される実施形態の範囲を過度に限定するよう意図されていない。多くの変形、代替手段、および変更が可能である。例えば、代替の実施形態では、分散環境６００は、より多くの、またはより少ない、クラウド環境を含んでよい。クラウド環境は、より多くの、またはより少ない、システムおよびコンポーネントを含んでもよく、あるいはシステムおよびコンポーネントの異なる構成または配置を有してよい。図６に示されたシステムおよびコンポーネントは、それぞれのシステムの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）において、ハードウェアを使用して、またはこれらの組合せで実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。

【０１３４】
マルチクラウド制御プレーン（ＭＣＣＰ）
図７は、一部の実施形態による、マルチクラウド制御プレーン（ＭＣＣＰ）の高レベルのアーキテクチャを示している。図７に示されているように、高レベルのアーキテクチャ７００は、第１のクラウドサービスプロバイダ（例えば、ＯＣＩ）７２０によって提供された第１のクラウド環境、および第２のクラウドサービスプロバイダ７１０（すなわち、Azure）によって提供された第２のクラウド環境を含む。第１のクラウド環境７２０は、第１のクラウド環境７２０のユーザに複数のサービスを提供する第１のクラウドインフラストラクチャ７２０Ａを含む。さらに、第１のクラウド環境７２０は、第１のクラウドインフラストラクチャ７２０Ａ（例えば、Oracleクラウドインフラストラクチャ（ＯＣＩ））のサービスを他のクラウド環境（例えば、第２のクラウドインフラストラクチャ７１０Ａ）のユーザに配信する能力をプロビジョニングするマルチクラウドインフラストラクチャ７２０Ｂを含む。マルチクラウドインフラストラクチャ７２０Ｂは、クラウド環境間の単純な統合をもたらしながら、ユーザが、ユーザのネイティブなクラウド環境のユーザ体験にできるだけ近いユーザ体験を伴って、他のクラウド上のサービス（例えば、Oracle PaaSサービス）にアクセスすることを可能にする。
【０１３５】
第２のクラウドインフラストラクチャ７１０Ａは、第２のクラウドポータル７１１、アクティブディレクトリ７１２、リソースマネージャ７１３、顧客サブスクリプション７１５、第１のクラウドプロバイダのサブスクリプション７１７を含む。第２のクラウドポータル７１１は、第２の環境７１０の顧客がログインし、クラウドのデプロイメントおよびインスタンスを管理することができる、集中型のアクセスポイントである。第２のクラウドポータルが、第２のクラウドインフラストラクチャによって提供された監視サービスおよび操作サービスの両方の選択肢を提供してよいということに注意する。アクティブディレクトリ７１２は、エンドユーザのアイデンティティおよびアクセス権限を管理する能力を管理者に提供する、第２のクラウドインフラストラクチャ７１０Ａによって提供されたサービスである。そのサービスは、コアディレクトリ、アクセス管理、およびアイデンティティ保護を含んでよい。リソースマネージャ７１３は、第２のクラウドインフラストラクチャのデプロイメントおよび管理サービス、すなわち、顧客サブスクリプション７１５においてデプロイされるリソースに関する操作（例えば、作成、更新、削除など）を実行するための、ユーザに提供する管理レイヤである。顧客サブスクリプションが、顧客のアプリケーションがデプロイされて実行される仮想ネットワーク（ＶＮＥＴ：virtual network）と呼ばれることもあるということに注意する。第２のクラウドインフラストラクチャ７１０Ａ内の第１のクラウドプロバイダ７１７のサブスクリプションは、第２のクラウドインフラストラクチャ７１０Ａと確立される（例えば、オンプレミスの場所から、外部クラウド環境からの）ネットワーク接続をプロビジョニングするエクスプレスルートならびにハブおよびスポークＶＮＥＴを含む。そのような接続が、パブリックインターネットを介してルーティングされなくてよく、それによって、さらなる信頼性、より速い速度、一貫性のある待ち時間、およびより高いセキュリティをユーザにもたらすということに注意する。
【０１３６】
第１のクラウドインフラストラクチャ７２０Ａは、制御プレーン７２４、顧客のテナンシ７２６、およびマルチクラウドインフラストラクチャ７２０Ｂを含む。第１のクラウドインフラストラクチャ７２０Ａの制御プレーン７２４は、クラウド環境にわたって管理およびオーケストレーションを提供する第１のクラウド環境のネイティブな制御プレーンである。制御プレーン７２４では、構成ベースラインが設定され、ユーザおよびロールのアクセスがプロビジョニングされ、アプリケーションが存在するため、アプリケーションが関連するサービスと共に実行され得る。マルチクラウドインフラストラクチャ７２０Ｂは、マルチクラウドプラットフォームデータプレーン７２２、およびマルチクラウドプラットフォームデータプレーン７２８を含む。前述したように、マルチクラウドインフラスト

ラクチャ７２０Ｂは、クラウド環境間の単純な統合をもたらしながら、他のクラウド環境（例えば、第２のクラウド環境７１０）のユーザが、ユーザのネイティブなクラウド環境（例えば、第２のクラウド環境７１０）のユーザ体験にできるだけ近いユーザ体験を伴って、第１のクラウド環境によって提供されたサービスにアクセスするために、プロビジョニングする。

【０１３７】

図７のＭＣＣＰアーキテクチャは、第２のクラウドインフラストラクチャ７１０内で認証されたユーザが、マルチクラウドインフラストラクチャ７２０Ｂを介して公開される第１のクラウドインフラストラクチャ７２０のリソースに対して制御プレーンの操作を実行することを許可する、マルチクラウドコンソール７２１（第２のクラウドポータル７１１と異なる）をさらに含む。一部の実装では、図７に示されているように、マルチクラウドコンソール７２１に送信されたすべてのユーザ７０５の要求は、第１のクラウド環境に含まれているマルチクラウドインフラストラクチャに向けられる。ユーザ７０５が、第１のクラウドインフラストラクチャによって提供されたリソースに関する要求（例えば、ＣＲＵＤ要求）をマルチクラウドコンソール７２１に直接送信できるということが理解される。マルチクラウドコンソール７２１は、第２のクラウドインフラストラクチャ内でローカルに使用される構文または形式に類似する構文または形式を有する要求を処理するように構成される。言い換えると、マルチクラウドコンソール７２１は、第２のクラウドインフラストラクチャ７１０Ａに含まれている第２のクラウドポータル７１１に類似するルックアンドフィールを有するだけでなく、類似する用語を使用する。一部の実装では、第２のクラウドコンソール７１１内で、ユーザをマルチクラウドコンソール７２１に向けるリンク（例えば、ウェブリンク）が提供されてよい。

【０１３８】

第１のクラウドインフラストラクチャ７２０Ａに含まれているマルチクラウドインフラストラクチャ７２０Ｂは、権限モジュール７２２Ａ、プロキシモジュール７２２Ｂ、プラットフォームサービスモジュール７２２Ｃ、クラウドリンクアダプタ７２２Ｄ、アダプタ１、アダプタ２、アダプタ３、およびアダプタ４を含んでいるアダプタのプール７２２Ｅ、ならびにネットワークリンクアダプタ７２２Ｆなどの、複数のマイクロサービスを含む。アダプタのプール７２２Ｅは、エクサデータクラウドサービスアダプタ、自律的データベース共有アダプタ、自律的データベース専用アダプタ、および仮想マシンデータベースアダプタなどのアダプタを含むことができる。

【０１３９】

アダプタのプール７２２Ｅに含まれているアダプタの各々は、（第１のクラウドインフラストラクチャ７２０Ａによって提供された）固有の基盤になるリソースのセットを、他のクラウド環境（例えば、第２のクラウド環境）のユーザに公開する役割を担う。特に、アダプタのプール７２２Ｅ内のアダプタの各々は、第１のクラウドインフラストラクチャ７２０Ａによって提供された特定の製品またはリソースにマッピングされる。実際のリソースが、第１のクラウドインフラストラクチャのネイティブな制御プレーン７２４によって作成されるということに注意する。例えば、ＤＢａａＳ（database as a service）に関して、制御プレーン７２４に含まれているＤＢａａＳ制御プレーンは、第１のクラウド環境の顧客のテナンシ７２６内のエクサデータベースリソースをインスタンス化するように構成される。

【０１４０】

マルチクラウドインフラストラクチャ７２０Ｂによって受信された着信要求は、認証およびアクセス制御を実行するために、権限モジュール７２２Ａによって処理される。各要求は、第２のクラウドインフラストラクチャ内のユーザのアカウントに関連付けられたトークンを含む。権限モジュールは、このトークンを抽出し、アクティブディレクトリ７１２（すなわち、第２のクラウドインフラストラクチャ７１０Ａのアイデンティティプロバイダシステム）と共に、トークンの妥当性を確認する。妥当性確認の成功時に、権限モジュール７２２Ａは、ユーザに関連付けられたロール（すなわち、権限のセット）をチェッ

クしてよい。ロールが、ロールに対して許可されている１つまたは複数のタスク／操作に関連付けられてよいということに注意する。１つの実施形態によれば、権限モジュール７２２Ａは、ＭＣＣＰへの着信要求を認証する役割、およびトークンに関連付けられたロールに基づいて、ユーザが要求された操作を実行することを許容されている場合に許可する役割を担う。一部の実装では、権限モジュール７２２Ａは、サービスプラットフォーム（すなわち、第１のクラウドインフラストラクチャに関連付けられたＳＰＬＡＴ）のカスタム認証機能を利用することによって、前述の認証プロセスを実行してよい。ＳＰＬＡＴは、着信要求を受け取って権限モジュール７２２Ａに転送し、権限モジュール７２２Ａは、着信要求をさらに構文解析して、許可決定を判定し、成功メッセージまたは失敗メッセージをＳＰＬＡＴに返す。成功時に、この要求がＳＰＬＡＴによってルーティングプロキシ７２２Ｂに渡され、一方、失敗時に、ＳＰＬＡＴは、エラー応答を呼び出し元に直接返す。

【０１４１】

マルチクラウドインフラストラクチャ７２０Ｂに含まれているプロキシモジュール７２２Ｂ（ルーティングプロキシモジュールとも呼ばれる）は、マルチクラウドコンソール７２１から着信要求を受信し、この要求を、アダプタのプール７２２Ｅに含まれている特定のアダプタにルーティングするコンポーネントである。１つの実施形態によって、プロキシモジュール７２２Ｂは、第１のクラウドインフラストラクチャのサービスプラットフォーム（すなわち、ＳＰＬＡＴ）から事前に認証された要求を受け取り、着信要求に含まれている経路情報に基づいて、この要求を適切なアダプタにルーティングする。一部の実装では、プロキシモジュール７２２Ｂは、（着信要求から）サービスのプロバイダに対応する識別子を抽出し、この要求を、アダプタのプール７２２Ｅ内の適切なアダプタにルーティングする。

【０１４２】

マルチクラウドインフラストラクチャ７２０Ｂに含まれているクラウドリンクアダプタ７２２Ｄは、第１のクラウドインフラストラクチャによって提供されたリソースのライフサイクル操作を処理する役割を担う。クラウドリンクアダプタ７２２Ｄは、第２のクラウドインフラストラクチャのアクティブディレクトリテナント（および関連付けられたサブスクリプション）と第１のクラウドインフラストラクチャ内のユーザの対応するテナンシ／アカウントの間のマッピング（またはサインアッププロセスで作成される関係）を作成するように構成される。言い換えると、クラウドリンクアダプタ７２２Ｄは、第２のクラウドインフラストラクチャ内のユーザのアカウントに関連付けられた第２の識別子への、第１のクラウドインフラストラクチャ内のユーザのテナンシに関連付けられた第１の識別子のマッピングを生成する。

【０１４３】

一部の実装では、クラウドリンクアダプタ７２２Ｄは、外部のクラウド識別子（例えば、第２のクラウドインフラストラクチャ内のユーザのアカウントに関連付けられた第２の識別子）と（第１のクラウドインフラストラクチャ内のユーザのテナンシに関連付けられた）第１の識別子の間の変換を実行し、マルチクラウド制御プレーン７２２を通過する操作が、第１のクラウドインフラストラクチャ内の適切な基盤になるリソースにマッピングされることを可能にする。一部の実施形態では、クラウドリンクアダプタは、前述のマッピング情報を格納するために、データオブジェクトを生成する。さらに、クラウドリンクアダプタ７２２Ｄは、データオブジェクトに関連付けられているリソースプリンシパルも生成する。リソースプリンシパルには、要求に含まれているトークン（およびその関連付けられたロール）に基づいて１つまたは複数の許可が割り当てられる。第１のクラウドインフラストラクチャによって提供された下流のサービスへのアクセスは、リソースプリンシパルに基づいて、第２のクラウドインフラストラクチャからのユーザによって達成される。クラウドリンクアダプタ７２２Ｄは、データオブジェクトおよび関連付けられたリソースプリンシパルを、第１のクラウドインフラストラクチャ内のユーザのテナンシのルート区画に格納してよい。代替的または追加的に、クラウドリンクアダプタ７２２Ｄは、デ

ータオブジェクトおよびリソースプリンシパルを、マルチクラウドインフラストラクチャに含まれている他のアダプタによるシームレスなアクセスのために、マルチクラウドインフラストラクチャのプラットフォームサービスモジュール７２２Ｃにローカルに維持してもよい。

【０１４４】

ネットワークリンクモジュール（ネットワークアダプタとも呼ばれる）７２２Ｆは、（第２のクラウドインフラストラクチャ内の）顧客サブスクリプション７１５と（第１のクラウドインフラストラクチャ内の）対応する顧客のテナンシ／アカウント７２６の間のネットワークリンクを作成する役割を担う。一部の実施形態によって、ネットワークリンクモジュール７２２Ｆは、（プラットフォームサービスモジュール７２２Ｃから）トークンを取得し、（１）マルチクラウドプラットフォームデータプレーン７２８と顧客のテナンシ７２６の間の（第１のクラウド環境内の）第１のピアリング関係、および（２）第２のクラウドインフラストラクチャに含まれている顧客サブスクリプション７１５と第１のクラウドサービスプロバイダのサブスクリプション７１７の間の（第２のクラウド環境内の）第２のピアリング関係を作成する。

【０１４５】

ネットワークリンクモジュール７２２Ｆは、第１のクラウド環境と第２のクラウド環境の間のネットワーク接続を確立するようにも構成され、すなわち、ネットワークリンクモジュール７２２Ｆは、相互接続７１９を、２つのクラウド環境を通信可能に結合するように構成することができる。２つのクラウド環境間にネットワークリンクを形成すると、顧客のサブスクリプションにおいて（例えば、第２のクラウドインフラストラクチャのＶＮＥＴ内で）実行されるアプリケーションが、リソース（例えば、第１のクラウドインフラストラクチャの顧客のテナンシ７２６にデプロイされているエクサデータベースリソース）にアクセスできるということが理解される。さらに、図７に示されているように、テナンシ７２６内で、遠隔測定の機能が提供されている。そのような機能は、顧客のテナンシにデプロイされたリソースおよびそれらの各使用に関連する、ログ、指標、および他の性能パラメータを維持することに関連している。一部の実施形態によれば、ＭＣＣＰは、第１のクラウド環境内の異なるリソースに関連付けられたログおよび指標をミラーリングし、指標、ログ、イベントなどを、さらなる処理のために、例えばダッシュボードに（例えば、第２のクラウド環境の顧客サブスクリプション７１５に含まれているアプリケーションインサイトモジュールに）公開する。

【０１４６】

一部の実施形態によって、マルチクラウドインフラストラクチャに含まれているプラットフォームサービスモジュール７２２Ｃは、第２のクラウドインフラストラクチャに提供された第１のクラウドインフラストラクチャのサービスに関連付けられた認証情報を格納するように構成される。プラットフォームサービスモジュール７２２Ｃは、アダプタが、第１のクラウドインフラストラクチャのネイティブな制御プレーン７２４と通信できるように、例えば、アダプタ７２２Ｅのプールに含まれているさまざまなアダプタのトークン／リソースプリンシパルを提供する。一部の実施形態によって、プラットフォームサービスモジュール７２２Ｃは、次のようなタスクを実行するために、さまざまなアダプタによって呼び出されるＡＰＩを公開する。

・（第２のクラウドインフラストラクチャによって発行された）最小限に範囲指定されたアクセストークンをアダプタに販売する。例えば、ネットワークアダプタ７２２Ｆは、前述のネットワークピアリング操作を実行するために、アクセストークンを必要とする。

・下流のサービスを呼び出して第１のクラウドインフラストラクチャの顧客のテナンシにリソースを作成するためにアダプタが使用する、リソースプリンシパルを提供する。

・第１のクラウドインフラストラクチャから第２のクラウドインフラストラクチャへの可観測性データ（ログ、指標、イベント）の複製を引き起こす。

【０１４７】

前述したように、アダプタのプールは複数のアダプタを含み、それらのアダプタの各々

は、第１のクラウドインフラストラクチャの固有の基盤になるリソースのセットを第２のクラウドインフラストラクチャのユーザに公開する役割を担い、すなわち、各アダプタは、第１のクラウド環境によって提供された特定の製品またはリソースにマッピングされる。例えば、エクサデータベースアダプタは、第２のクラウドインフラストラクチャのユーザがエクサデータベースリソースを作成して利用するための、プロキシとして機能する。エクサデータベースは、データベースを実行するためのインフラストラクチャを提供するハードウェアとソフトウェアの事前に構成された組合せである。一部の実施形態によって、エクサデータベースは、（ａ）エクサデータインフラストラクチャ（すなわち、ハードウェア）、（ｂ）ＶＭクラウドクラスタ、（ｃ）コンテナデータベース、および（ｄ）プラガブルデータベースという、リソースのスタックを備える。一部の実施形態によれば、マルチクラウドインフラストラクチャは、積み重ねられたインフラストラクチャのレベルの各々を分析する能力を（第２のクラウドインフラストラクチャのユーザに）提供する。さらに、ＭＣＣＰは、ユーザが（マルチクラウドコンソール７２１を介して）ワークフローの作成コマンドを単に発行するための柔軟性を提供し、その後、ＭＣＣＰは、スタックの各レベルで、個別のリソースの自動作成を実行する。図７に示されているように、アダプタのプール７２２Ｆは、４つの異なるアダプタを含んでいるが、これがＭＣＣＰアーキテクチャ７００の範囲を全く制限していないということが、理解される。ＭＣＣＰアーキテクチャは、他のアダプタ、例えば、クラウドサービスプロバイダの要求に基づいて、特定のクラウドサービスプロバイダによる使用を目的とする専用アダプタを含んでよい。

【０１４８】

図８Ａおよび図８Ｂは、一部の実施形態による、異なるクラウド環境内の２つのユーザアカウントをリンクするための例示的なフロー図を示している。２つのユーザアカウントは、第１のクラウドインフラストラクチャ内の第１のユーザアカウント（例えば、テナンシ）および第２のクラウドインフラストラクチャ内の第２のユーザアカウントに対応してよい。図８Ａは、２つのユーザアカウントをリンクするプロセスを示しており、最初に、ユーザのテナンシが第１のクラウドインフラストラクチャ内に作成され、次に、第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクされる。図８Ｂは、２つのユーザアカウントをリンクするプロセスを示しており、第１のクラウドインフラストラクチャ内のユーザのテナンシがすでに作成されており、すなわち、テナンシがすでに存在する。

【０１４９】

図８Ａは、システム管理者などの、顧客を表すユーザが、第１のクラウドインフラストラクチャにおいて提供されたサービスにサインアップするために、第２のクラウドインフラストラクチャから（第１のクラウドインフラストラクチャに含まれている）マルチクラウドインフラストラクチャへの呼び出しを行うときに実行される、データフローを示している。第２のクラウドインフラストラクチャのユーザが第１のクラウドインフラストラクチャ内でアカウントを開くため、および第１のクラウドインフラストラクチャ内のユーザのアカウントを第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクするために、特殊なコンソール（本明細書では、マルチクラウドコンソールと呼ばれる）が提供されてよい。第１および第２のクラウドインフラストラクチャ内のアカウントをリンクすることによって、（第２のクラウドインフラストラクチャからの）ユーザが、第１のクラウドインフラストラクチャによって提供された１つまたは複数のサービスを利用できるようになるということに注意する。ある実装では、ユーザは、マルチクラウドコンソールを使用してサービスにサインアップする。サインアップに応答して、ユーザがマルチクラウドコンソールにログインできるようにするＵＲＬが、ユーザに送信されてよい。マルチクラウドコンソールは、第２のクラウドインフラストラクチャのＵＩおよびＡＰＩに類似するＵＩおよびＡＰＩを公開する。

【０１５０】

マルチクラウドコンソールは、第２のクラウドインフラストラクチャのユーザが、第１のクラウドインフラストラクチャ内でアカウントを開くこと、ならびに第１および第２の

クラウドインフラストラクチャ内のユーザアカウントをさらにリンクすることを可能にする、ユーザ選択可能な選択肢を提供するさまざまなＵＩ（例えば、ＧＵＩ）を提供してよい。例えば、マルチクラウドコンソールは、ユーザが第１のクラウドインフラストラクチャ内でアカウント／テナンシを作成すること、および（第１のクラウドインフラストラクチャ内の）ユーザのアカウントを第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクすることを可能にする、サインアップＵＩを提供してよい。サインアップ／リンク要求に応答して引き起こされた処理が完了した後に、それぞれのクラウドインフラストラクチャ内のユーザのアカウントが一緒にリンクされる。この処理の一部として、マルチクラウドコンソールは、ユーザ（例えば、システム管理者）が、第２のクラウドインフラストラクチャにログインし、（ａ）（第１のクラウドインフラストラクチャ内の）ユーザのアカウントの作成を要求すること、およびユーザのアカウントをリンクすること、または（ｂ）ユーザが第１のクラウドインフラストラクチャ内ですでに保有しているアカウントの場合、ユーザの第１のクラウドインフラストラクチャのアカウントがユーザの第２のクラウドインフラストラクチャのアカウントにリンクされることを要求することを可能にする。

【０１５１】

したがって、ある使用事例では、次の２つの可能性がある。（ａ）ユーザが、第１のクラウドインフラストラクチャ内で既存のアカウントまたはテナンシをすでに保有しており、ユーザが、現在、マルチクラウドコンソールのサインアップＵＩを介して、ユーザのアカウント間にリンクが作成されることを要求している（この処理に関する詳細が、次に、図８Ｂを参照して説明される）、または（ｂ）ユーザが、第１のクラウドインフラストラクチャ内の新しいアカウントの作成、および第２のクラウドインフラストラクチャ内のユーザのアカウントとの新たに作成されたアカウントのリンクの両方を要求する。この処理に関する詳細が、次に、図８Ａを参照して説明される。アカウントのリンクは、ユーザが第２のクラウドを介して第１のクラウド内のリソースを使用することを可能にするということが、理解される。例えば、第２のクラウドを介して、ユーザは、第１のクラウド内でリソースが作成されるか、またはプロビジョニングされることを要求すること、第１のクラウド内のリソースを利用して管理すること、第１のクラウド内のリソースを削除することなどができる。

【０１５２】

図８Ａに示されているように、ステップ１で、第１のクラウドインフラストラクチャ内でユーザの新しいアカウントが作成され、第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクされることを要求する、マルチクラウドコンソール（例えば、マルチクラウドコンソールのサインアップＵＩ）に提供されたユーザの入力に応答して、新しいアカウントを作成するために、マルチクラウドコンソールによって、（第１のクラウドインフラストラクチャ内の）アカウントサービスへの呼び出しが行われる。この呼び出しが、第２のクラウドインフラストラクチャによって生成されるトークンを含むということに注意する。第２のクラウドインフラストラクチャによって生成され、アカウントサービスへの呼び出しに含まれるトークンは、第１のクラウドインフラストラクチャ内で作成されたアカウントまたはテナンシが第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクされることを可能にする。

【０１５３】

ステップ２で、ユーザの新しいアカウントを設定するための処理の一部として、アカウントサービスは、マルチクラウド制御プレーンに含まれている権限／プロキシモジュール（例えば、図７のマルチクラウドインフラストラクチャに含まれている権限モジュール７２２Ａ）への呼び出しを行い、トークンの妥当性を確認してよい。権限／プロキシモジュールは、（図７を参照して前に説明されたように）トークンの妥当性を確認し、トークンの妥当性確認の成功時にのみ、さらに処理が続行してよい。トークンの妥当性確認の成功時に、アカウントサービスは、第１のクラウドインフラストラクチャ内のユーザの新しいアカウントを作成する。新しいアカウントを作成することの一部として、ネイティブユー

ザが作成され、新たに作成されたアカウントに関連付けられてよい。しかし、このネイティブユーザの認証情報が使用されないということに注意する。むしろ、第１のクラウドインフラストラクチャ内の（第２のクラウドインフラストラクチャからの）アカウントおよびそのリソースを管理するために、第２のクラウドインフラストラクチャ内のユーザのアイデンティティが使用される。

【０１５４】

第１のクラウドインフラストラクチャ内のアカウントサービスによって新しいアカウントが正常に作成された後に、ステップ３で、アカウントサービスは、（マルチクラウドインフラストラクチャに含まれている）クラウドリンクアダプタへの呼び出しを行い、第２のクラウドインフラストラクチャ内のユーザのアカウントと第１のクラウドインフラストラクチャ内の新たに作成されたアカウントの間のリンク（クラウドリンクとも呼ばれる）を作成する。ある実装では、クラウドリンクアダプタが、ＡＰＩをアカウントサービスに、およびマルチクラウドコンソールに公開する。これらのＡＰＩは、アカウントのリンクを要求するために、アカウントサービスによって（または、マルチクラウドコンソールによって）呼び出されてよい。一部の実装では、リンクを要求する呼び出しが、ユーザによって行われず、むしろ、アカウントサービスによって開始されるため、ステップ３の呼び出しにトークンが含まれていないということに注意する。この場合、クラウドリンクアダプタは、アカウントサービスが、ステップ１で受信されたトークンを使用してアカウントを設定するための処理の一部として、ユーザに対して必要な認証をすでに実行しているということを信頼するため、別のトークンを必要とする別の認証を行わない。

【０１５５】

一部の実装では、２つのアカウントをリンクするためにクラウドリンクアダプタによってステップ３で実行される処理は、以下を含む。

（ａ）クラウドリンクアダプタが、リンクされている２つのアカウントを識別するメタデータ情報を格納するためのデータオブジェクト（本明細書では、クラウドリンクリソースオブジェクトとも呼ばれる）を作成する。例えば、データオブジェクトは、第１のクラウドインフラストラクチャ内に作成されたテナンシ（すなわち、アカウント）に関連付けられた第１の識別子、および第２のクラウドサービスプロバイダを使用してユーザのアカウントに関連付けられた第２の識別子のマッピングを含んでいるメタデータ情報を格納する。

（ｂ）クラウドリンクアダプタが、第１のクラウドインフラストラクチャ側でリソースを格納し、含むための新しい区画を作成し、ユーザは、この区画を、マルチクラウドコンソールを使用して管理することができる／管理する。一部の実装では、クラウドリンクリソースオブジェクトは、第１のクラウドインフラストラクチャ内の顧客のアカウントのルートに作成される。

（ｃ）クラウドリンクアダプタが、第２のクラウドインフラストラクチャのユーザによって使用されるのが望ましいリソースに関して、新しいリソースプリンシパル（本明細書では、クラウドリンクリソースプリンシパルと呼ばれる）を作成する。

（ｄ）クラウドリンクアダプタが、アクティブディレクトリ（例えば、図７に示されているような第２のクラウドインフラストラクチャのアクティブディレクトリ７１２）への第１のクラウドインフラストラクチャ内のドメインのリンクを容易にする１つまたは複数のフェデレーション設定を実行してよい。第１のクラウドインフラストラクチャおよび第２のクラウドインフラストラクチャのアカウントをフェデレートするプロセスは、第２のクラウドインフラストラクチャ内のユーザ／ユーザのグループが第１のクラウドインフラストラクチャ内で認証されること、および第１のクラウドインフラストラクチャからのユーザ／グループが第２のクラウドインフラストラクチャ内へ認証されることを可能にする。

【０１５６】

ある実装では、第２のクラウドインフラストラクチャのアカウントにおけるユーザの認証情報／トークンに基づいて、許可がクラウドリンクリソースプリンシパルに関連付けられる。ユーザが、マルチクラウドコンソールを使用して新しいアカウントを要求するか、

または第１のクラウドインフラストラクチャ内のユーザのアカウントが第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクされることを要求するときに、ユーザによって、リソースプリンシパルを設定することに対する同意が提供される。さらに、ステップ４に示されているように、ユーザが第２のクラウドインフラストラクチャから下流のサービス（例えば、第１のクラウドインフラストラクチャによって提供された１つまたは複数のサービス）を利用できるようにするために、クラウドリンクリソースプリンシパルが下流のサービスに送信される。

【０１５７】

図８Ｂを参照すると、第１のクラウドインフラストラクチャ内の既存のアカウントまたはテナンシを第２のクラウドインフラストラクチャ内のユーザのアカウントにリンクすることに関連する処理が示されている。図８Ｂに示されているように、ユーザは、マルチクラウドコンソールによって提供されたサインアップＵＩを介して、第１のクラウドインフラストラクチャおよび第２のクラウドインフラストラクチャ内のユーザのアカウントがリンクされることを要求する。それに応じて、ステップ１で、マルチクラウドコンソールがクラウドリンクアダプタへの呼び出しを行い、アカウントをリンクする。そのような呼び出しは、クラウドリンクアダプタによってサインアップＵＩに公開されたＡＰＩのうちの１つを使用して行われてよい。ある実装では、ステップ１でクラウドリンクアダプタに渡される情報は、第２のクラウドインフラストラクチャ内のユーザのアカウントおよびさらに第１のクラウドインフラストラクチャ内のユーザのアカウントを識別する情報、第２のクラウドインフラストラクチャによって発行されたトークンなどを含む。

【０１５８】

ステップ２で、クラウドリンクアダプタは、マルチクラウドインフラストラクチャに含まれている権限／プロキシモジュールへの呼び出しを行い、ステップ１で受信されたトークンを認証する。この認証の一部として、権限／プロキシモジュールは、要求を行っているユーザが、第２のクラウドインフラストラクチャ側でリンク要求を行うための十分な権限を持っているかどうかを判定する。この妥当性確認の一部として、第２のクラウドインフラストラクチャ側でのロールおよび許可設定がチェックされてよい。ユーザの妥当性確認が成功することに応答して、クラウドリンクアダプタは、ユーザのために前に作成されたデータオブジェクトから、ユーザによって利用されるのが望ましいリソースに関連付けられたリソースプリンシパルを取り出す。さらに、ステップ３に示されているように、ユーザが第２のクラウドインフラストラクチャから下流のサービス（例えば、第１のクラウドインフラストラクチャによって提供された１つまたは複数のサービス）を利用できるようにするために、クラウドリンクリソースプリンシパルが下流のサービスに送信される。

【０１５９】

図９は、一部の実施形態による、マルチクラウド制御プレーン（ＭＣＣＰ）のコンポーネントを示す例示的なシステム図を示している。ＭＣＣＰ９００は、サービスプラットフォーム（ＳＰＬＡＴ）９１０、ルーティングプロキシ９１５、クラウドリンクアダプタ９２０、データベースアダプタ９２５、ネットワークアダプタ９３０、およびＭＣＣＰプラットフォーム９３５を含む。図８Ａおよび図８Ｂを参照して上で説明されたように、ユーザがサインアッププロセスを正常に完了すると、ユーザは、マルチクラウドコンソール９０５を利用して、第１のクラウドインフラストラクチャ内のユーザのテナンシにおけるリソースにアクセスするか、リソースを作成するか、または更新するためのコマンドを発行してよい。説明の目的で、以下では、ユーザがマルチクラウドコンソールを利用して、エクサデータベースリソースを作成する要求を発行する状況が説明されている。

【０１６０】

一部の実装では、ユーザが、マルチクラウドコンソール９０５にアクセスし、ログイン情報、例えば、第２のクラウドインフラストラクチャ内のユーザの認証情報を提供する。マルチクラウドコンソール９０５は、例えば、リソースの作成、リソースへのアクセス、リソースの更新などの、複数の選択肢を提供する。そのような選択肢は、マルチクラウドコンソール９０５内の選択可能なアイコン（例えば、ボタン）の形態でユーザに提供され

てよい。ユーザが（例えば、リソースを作成するための）選択を実行すると、サービスプラットフォーム９１０へのＡＰＩ呼び出しが引き起こされる。サービスプラットフォーム９１０に対して行われる要求が、第１のクラウドインフラストラクチャに関するネイティブな呼び出しでないということが理解される。むしろ、この呼び出しは、第２のクラウドインフラストラクチャ内のユーザに関連付けられたトークンを含む許可ヘッダーを含んでいるＲＥＳＴ型の呼び出しである。

【０１６１】

トークンを含んでいるＲＥＳＴ呼び出しが、認証動作およびアクセス制御動作を実行するルーティングプロキシモジュール９１５にさらに転送される。一部の実施形態によれば、ルーティングプロキシモジュール９１５は、ＲＥＳＴ呼び出しに含まれているトークンを抽出することによって、認証動作を実行する。ルーティングプロキシモジュール９１５は、署名（要求に署名するために使用される）を、第２のクラウドインフラストラクチャの公開されている署名と比較することによって、トークンの妥当性を確認し、要求が第２のクラウドインフラストラクチャに関連付けられた有効な顧客から生じていることを保証する。さらに、ルーティングプロキシモジュール９１５は、ロール、すなわち、トークンに関連付けられた権限をチェックしてもよく、例えば、ロールがエクサデータＤＢ管理者に対応するかどうかなどをチェックしてもよい。ロールに基づいて、ルーティングプロキシモジュール９１５は、要求をＭＣＣＰフレームワーク９００に含まれている適切なアダプタにルーティングしてよい。

【０１６２】

１つの実施形態によれば、ルーティングプロキシモジュール９１５は、（トークンに関連付けられた）ロールを、公開されて（ＡＰＩ仕様の一部として）アダプタの各々に割り当てられたロールの事前に構成されたリストと比較する。例えば、トークンに関連付けられたロールが「エクサデータＤＢ管理者」に対応する場合、要求は、エクサデータベースを作成する要求として理解されてよく、したがって要求が、データベースアダプタ９２５に転送される。さらに、一部の実施形態によって、ルーティングプロキシモジュール９１５は、プロバイダＩＤ、要求されたリソースの種類などの、ＲＥＳＴ呼び出しに含まれている情報を分析してよく、分析された情報に基づいて、ルーティングプロキシモジュール９１５は、要求を適切なアダプタに転送してよい。

【０１６３】

一部の実装では、ルーティングプロキシモジュール９１５によって取得された要求は、リソースがデプロイされるべきである第１のクラウドインフラストラクチャ内のユーザのテナンシを識別する情報を含まなくてよい。したがって、ルーティングプロキシモジュール９１５は、クラウドリンクアダプタ９２０と通信し、第１のクラウドインフラストラクチャ内のユーザのテナンシへの、第２のクラウドインフラストラクチャ内のユーザのアカウントのマッピング情報を取得する。マッピング情報が存在する場合、ルーティングプロキシモジュール９１５は、第１のクラウドインフラストラクチャ内のユーザのテナンシに関する情報を取得し、この情報をデータベースアダプタ９２５に渡す。このようにして、データベースアダプタ９２５は、リソースが作成／デプロイされるべきである第１のクラウドインフラストラクチャ内のユーザのテナンシを認識する。しかし、クラウドリンクアダプタ９２０が、マッピング情報が存在しないということを決定した場合、ルーティングプロキシモジュール９１５は、データベースリソースを作成する要求に対する応答として、ユーザに返信される「許可されないアクセス」メッセージを単に発行してよい。

【０１６４】

一部の実装では、クラウドリンクアダプタ９２０が、リンクされている２つのアカウントを識別するメタデータ情報を格納するためのデータオブジェクト（本明細書では、クラウドリンクリソースオブジェクトと呼ばれる）を作成するということに注意する。例えば、データオブジェクトは、第１のクラウドインフラストラクチャ内のテナンシ（すなわち、アカウント）に関連付けられた第１の識別子、および第２のクラウドサービスプロバイダを使用してユーザのアカウントに関連付けられた第２の識別子のマッピングを含んでい

るメタデータ情報を格納する。さらに、クラウドリンクアダプタ９２０が、第２のクラウドインフラストラクチャのユーザによって作成／管理されるのが望ましいリソース（例えば、データベース）に関して、リソースプリンシパル（本明細書では、クラウドリンクリソースプリンシパルと呼ばれる）も作成する。クラウドリンクアダプタ９２０は、データオブジェクトおよびリソースプリンシパルを、第１のクラウドインフラストラクチャ内のユーザのテナンシのルート区画内で維持してよい。一部の実施形態では、クラウドリンクアダプタ９２０は、ＭＣＣＰプラットフォーム９３５内のデータオブジェクトおよび／またはリソースプリンシパルをローカルに維持してもよい。

【０１６５】

一部の実施形態では、データベースアダプタ９２５は、ネットワークアダプタ９３０と通信し（またはネットワークアダプタ９３０に指示し）、第２のクラウドインフラストラクチャ内のユーザのアカウントと第１のクラウドインフラストラクチャ内のユーザのテナンシの間のネットワークリンクを作成してよい。例えば、ネットワークアダプタ９３０は、第２のクラウドインフラストラクチャモジュール９４５内のネイティブなサービスから、ユーザに関連付けられたトークンを取得し、（１）ＭＣＣＰのデータプレーンと第１のクラウドインフラストラクチャ内のユーザのテナンシの間の（第１のクラウド環境内の）第１のピアリング関係、および（２）第２のクラウドインフラストラクチャに含まれているユーザのアカウントと第１のクラウドプロバイダのサブスクリプションの間の（第２のクラウド環境内の）第２のピアリング関係を作成してよい。

【０１６６】

ネットワークアダプタ９３０は、第１のクラウドインフラストラクチャと第２のクラウドインフラストラクチャの間のネットワーク接続を確立するようにも構成され、すなわち、ネットワークアダプタ９３０は、２つのクラウド環境を通信可能に結合する相互接続（例えば、図７の相互接続７１９）を構成することができる。第１のクラウドインフラストラクチャ内のユーザのテナンシと第２のクラウドインフラストラクチャ内のユーザのアカウントの間にネットワークリンクを形成すると、ユーザのサブスクリプション／アカウントにおいて実行されるアプリケーションが、リソース、例えば、第１のクラウドインフラストラクチャのテナンシにデプロイされたエクサデータベースにアクセスできるということが、理解される。さらに、ピアリング関係の作成は、第２のクラウドインフラストラクチャ内で、例えば、第２のクラウドインフラストラクチャ内のユーザのサブスクリプションにおいて実行されるダッシュボードアプリケーションにおいて、アクセスできるように、指標、例えば、データベース使用量指標をプロビジョニングする。

【０１６７】

一部の実装では、データベースアダプタ９２５は、ＭＣＣＰプラットフォーム９３５内でローカルに維持されているリソースプリンシパルを取得してよい。データベースアダプタ９２５は、（リソースプリンシパルを含んでいる）要求を、第１のクラウドインフラストラクチャ９４０に含まれている１つまたは複数の下流のサービスに送信し、第１のクラウドインフラストラクチャ内のユーザのテナンシにリソースを作成してよい。言い換えると、第１のクラウドインフラストラクチャ９４０に含まれている下流のサービスは、アイデンティティを利用し、すなわち、要求されたリソース（例えば、第１のクラウドインフラストラクチャ内のユーザのテナンシにおけるエクサデータベース）を作成／デプロイするためにＭＣＣＰプラットフォーム９３５から取得されたリソースプリンシパルを利用する。ユーザが、エクサデータベースを作成する要求を発行すると、ユーザは、ＭＣＣＰ９００を断続的にポーリングし、要求の状態を取得してよい。第１のクラウドインフラストラクチャ９４０の下流のサービスが、第１のクラウドインフラストラクチャ内のユーザのテナンシにリソースを作成し、ネットワークアダプタ９３０がピアリング関係を確立すると、ＭＣＣＰ９００は、要求の正常な完了に関してユーザに通知してよい。

【０１６８】

マルチクラウドネットワークサービス－ネットワークアダプタ

図７を参照すると、マルチクラウド制御プレーン７００のアーキテクチャは、（外部ク

ラウドサービスプロバイダによって提供されている）外部クラウド環境、例えば、第２のクラウド環境７１０の顧客が、（第１のクラウド環境に含まれている）マルチクラウドコンソール７２１およびマルチクラウドインフラストラクチャ７２０Ｂを利用することによって、第１のクラウド環境７２０内で提供されたリソース（例えば、データベースリソース）をデプロイすること、サービスを実行することなどを可能にする。一部の実装では、第１のクラウド環境と第２のクラウド環境の間のネットワーク接続は、第１のクラウド環境のサービスの提供（例えば、ＰａａＳの提供）を第２のクラウド環境の顧客に公開するように構成されて維持されるべきである。下で詳細に説明されるように、ネットワークアダプタ（例えば、図７のネットワークリンクコンポーネント７２２）は、そのようなネットワークに関連するリソースを処理する役割を担う。

【０１６９】

ある実施形態では、第１のクラウド環境と他のクラウド環境、例えば、第２のクラウド環境との間のネットワーク接続を構成して維持する役割を担うマルチクラウドネットワーク（ＭＣＮ：multi-cloud network）サービスが提供されている。ＭＣＮは、ＰａａＳの提供などのサービスを、他のクラウド環境の顧客にシームレスな方法で公開する。ＭＣＮサービスが、ネットワークアダプタコンポーネント７２２Ｆのように、図７のマルチクラウド制御プレーン７００のアーキテクチャに適合するということが理解される。一部の実施形態によれば、ＭＣＮサービスは、次のような役割を担う。

１．マルチクラウドプラットフォームと統合され、クラウド間仮想ネットワーク相互接続の抽象化として機能する、ネットワークリンクと呼ばれる顧客向けのＡＰＩオブジェクトを顧客に公開する。

２．Ｎ人の顧客間で共有される、外部クラウド環境と第１のクラウド環境の間の直接相互接続リンク（例えば、ExpressRoute、FastConnectなど）を構成して維持する。

３．顧客ごとのパケットプロセッサインスタンスを起動して監視し、外部クラウド環境と第１のクラウド環境の間のエンドツーエンドのパケットフローを可能にする。

４．外部クラウド環境および第１のクラウド環境内で任意のドメイン名システム（ＤＮＳ：domain name system）に関連するリソースを構成し、シームレスな名前解決を可能にする。

【０１７０】

名前が示唆するように、ネットワークリンクは、２つのクラウド環境を相互接続する抽象化である。例えば、ネットワークリンクは、第２のクラウド環境内の顧客の仮想ネットワークを、第１のクラウド環境内の顧客の仮想クラウドネットワーク（ＶＣＮ）に相互接続してよい。顧客がネットワークリンクを手動で設定する必要がある場合、顧客は、第２のクラウド環境のための相互接続（例えば、Express Route）を構成すること、第１のクラウド環境のための別の相互接続（例えば、Fast Connect）を構成すること、ダイナミックルーティングゲートウェイを構成すること、ゲートウェイ接続およびルートテーブルを構成することなどの、多数のタスクの責任を負うということが、理解される。そのようなタスクは、実際は、決してささいなことではなく、さらに、不十分な顧客満足体験を引き起こす。本開示の実施形態によって説明されるように、顧客の対話を最小限に抑えるか、または顧客の対話なしで、ネットワークリンク（および関連するネットワークリソース）を自動的に構成するマルチクラウドネットワーク（ＭＣＮ）サービスが提供されている。したがって、ＭＣＮサービスを利用することによって、顧客は、第１のクラウド環境のマルチクラウドインフラストラクチャによって提供されたネットワークリンクコンポーネントの内部について心配する必要がなく、ネットワークリンクを、単に、異なるクラウド環境内の顧客の仮想ネットワークとの間のトラフィックを可能にするブラックボックスとして使用する。さらに、異なるクラウド環境間で確立されたネットワークリンクが、極めて短い送信待ち時間を有する必要があることがあるということに注意する。これは、第１のクラウド環境にデプロイされたリソースが、オンライントランザクション処理イベントを処理するエクサデータベースリソースなどのリソースであることがあるという事実に起因する。そのようなイベントが最小限の待ち時間を要求するため、本開示のマルチク

ラウドネットワーク（ＭＣＮ）サービスは、異なるクラウド環境間で、短い送信待ち時間を有する高性能で高可用性のエンドツーエンドのネットワークリンクを確立することを信頼される。

【０１７１】

図１０は、ある実施形態による、ネットワークリンクコンポーネントの高レベルのブロック図を示している。特に、図１０は、第１のクラウド環境１００５と第２のクラウド環境１０１０の間に確立されているネットワークリンクコンポーネント１００７（本明細書では、マルチクラウドネットワークインフラストラクチャ（ＭＣＮＩ：multi-cloud network infrastructure）とも呼ばれる）を示している。図１０に示されているように、ネットワークリンクコンポーネント１００７は、顧客の仮想ネットワーク（ＶＮＥＴ）、例えば第２のクラウド環境１０１０に含まれているＶＮＥＴ１０２２と、顧客の仮想クラウドネットワーク（ＶＣＮ）１０１２、すなわち、第１のクラウド環境１００５内のＶＮＥＴとの間に確立される。したがって、（第１のクラウド環境１００５内の）顧客のＶＣＮ１０１２内でホストされたリソース１０１３（例えば、エクサデータベース）が、第２のクラウド環境１０１０内の顧客のＶＮＥＴ１０２２内でホストされている仮想マシン１０２３によってアクセス／利用されてよい。

【０１７２】

図１０に示されているように、第２のクラウド環境側で、ネットワークリンクコンポーネント１００７は、第２のクラウド環境１０１０に含まれている顧客のＶＮＥＴ１０２２とピアリングする（リーフＶＮＥＴとラベル付けされた）ＶＮＥＴ１０１９を含んでいる。顧客のＶＣＮ１０１２との間の任意のトラフィックが、このＶＮＥＴピアリングにつながれる。リーフＶＮＥＴ１０１９が、顧客への汎用「ネットワークリンクＶＮＥＴ」のように見えるということに注意する。第１のクラウド環境側で、ネットワークリンクコンポーネント１００７は、マルチクラウド接続１０１７という名前のダイナミックルーティングゲートウェイ（ＤＲＧ）接続を含む。一部の実装では、顧客は、顧客のＶＣＮ（例えば、顧客のＶＣＮ１０１２）を、ＶＣＮ接続を使用して顧客が所有するＤＲＧ１０１５に接続してよく、ＭＣＮＩ１００７が、マルチクラウド接続１０１７を介してこのＤＲＧ１０１５にリンクされる。（第２のクラウド環境１０１０に含まれている）顧客のＶＮＥＴ１０２２との間の任意のトラフィックが、ＶＣＮ接続につながれ、次に、ＤＲＧ内のマルチクラウド接続１０１７につながれるということに注意する。

【０１７３】

図１１～図１３を参照して下で説明されるように、ネットワークリンクコンポーネント１００７の一部が第１のクラウド環境１００５に含まれ、一方、ネットワークリンクコンポーネント１００７の他の一部が第２のクラウド環境１０１０に含まれる。さらに、ネットワークリンクコンポーネント１００７の目的のうちの１つが、第１のクラウド環境と第２のクラウド環境の間の相互接続を共有するために、マルチテナントトンネルインフラストラクチャを構築することであるということが理解される。マルチテナントのトラフィックが単一のクラウド間相互接続を共有するために、ネットワークリンクコンポーネント１００７が、例えばＧＥＮＥＶＥトンネルを使用することによって顧客のトラフィックをカプセル化／カプセル解除するように、トンネルをプロビジョニングするということに注意する。

【０１７４】

図１１を参照すると、ある実施形態による、ネットワークリンク構成の詳細なアーキテクチャ１１００が示されている。図１１に示されているように、ネットワークリンクが、第２のクラウド環境１１０５のリージョンを第１のクラウド環境１１３５のリージョンに通信可能に結合する。第２のクラウド環境１１０５のリージョンは、１つまたは複数の顧客のＶＮＥＴを含んでよい。例えば、第２のクラウド環境１１０５のリージョンは、２つの顧客のＶＮＥＴ、すなわち、顧客１のＶＮＥＴ１１０１および顧客２のＶＮＥＴ１１０２を含む。したがって、顧客のＶＮＥＴをホストしている第２のクラウド環境１１０５の一部は、顧客ドメイン１１５０Ａとして表される。同様に、第１のクラウド環境１１３５

のリージョンは、１つまたは複数の顧客のＶＣＮ（すなわち、顧客の仮想ネットワーク）を含んでよい。例えば、第１のクラウド環境１１３５のリージョンは、２つの顧客のＶＣＮ、すなわち、顧客１のＶＣＮ１１３１および顧客２のＶＣＮ１１３２を含む。したがって、顧客のＶＣＮをホストしている第１のクラウド環境１１３５の一部は、顧客ドメイン１１５０Ｃとして表される。

【０１７５】

一部の実施形態によれば、マルチクラウドネットワークインフラストラクチャ（ＭＣＮＩ）ドメイン１１５０Ｂ、すなわち、ネットワークリンクは、顧客の仮想ネットワークの対を通信可能に結合する。例えば、図１１に示されているように、（第２のクラウド環境１１０５のリージョンに含まれている）顧客１のＶＮＥＴ１１０１は、（第１のクラウド環境１１３５のリージョンに含まれている）顧客１のＶＣＮ１１３１と通信可能に結合される。同様の方法で、（第２のクラウド環境１１０５のリージョンに含まれている）顧客２のＶＮＥＴ１１０２は、（第１のクラウド環境１１３５のリージョンに含まれている）顧客２のＶＣＮ１１３２と通信可能に結合される。ＭＣＮＩドメイン１１５０がネットワークリンクドメインに対応し、点線１１６０と１１７０の間に配置されるということに注意する。より詳細には、ＭＣＮＩドメインは、第２のクラウド環境１１０５のリージョンに配置されている第１の部分、および第１のクラウド環境１１３５のリージョンに配置されている第２の部分を含む。

【０１７６】

一部の実装では、顧客の仮想ネットワーク（例えば、第２のクラウド環境１１０５のリージョン内の顧客１のＶＮＥＴ１１０１および第１のクラウド環境１１３５のリージョン内の顧客１のＶＣＮ１１３１）の各対が、マルチクラウドネットワーク（ＭＣＮ）サービスによって（第１のクラウド環境および第２のクラウド環境に）デプロイされている複数の仮想ネットワーク（本明細書では、リンク有効化仮想ネットワークと呼ばれる）を使用して通信可能に結合される。例えば、第１のリンク有効化仮想ネットワーク１１０３（リーフ１ＶＮＥＴとしてラベル付けされている）および第２のリンク有効化仮想ネットワーク１１０７（スポーク１ＶＮＥＴとしてラベル付けされている）が、第２のクラウド環境１１０５のリージョンにデプロイされ、顧客１のＶＮＥＴ１１０１に関連付けられる。さらに、第３のリンク有効化仮想ネットワーク１１２３（スポーク１ＶＣＮとしてラベル付けされている）が、第１のクラウド環境１１３５のリージョンにデプロイされ、顧客１のＶＣＮ１１３１に関連付けられる。同様の方法で、顧客２のＶＮＥＴ１１０２が、第２のクラウド環境１１０５のリージョンにデプロイされているリンク有効化仮想ネットワーク１１０４（リーフ２ＶＮＥＴとしてラベル付けされている）および別のリンク有効化仮想ネットワーク１１０６（スポーク２ＶＮＥＴとしてラベル付けされている）に関連付けられ、一方、顧客２のＶＣＮ１１３２が、異なるリンク有効化仮想ネットワーク１１２４（スポーク２ＶＣＮとしてラベル付けされている）に関連付けられる。したがって、図１１のアーキテクチャでは、顧客の仮想ネットワークの各対が、３つのリンク有効化仮想ネットワークに関連付けられる。

【０１７７】

さらに、第２のクラウド環境１１０５のリージョンは、第２のクラウド環境に含まれている異なる顧客の仮想ネットワーク間で共有されているハブＶＮＥＴ１１１０を含む。言い換えると、ハブＶＮＥＴ１１１０は、第２のクラウド環境１１０５のリージョンに含まれている複数の顧客のテナンシのトラフィックを処理する。同様に、第１のクラウド環境１１３５のリージョンは、第１のクラウド環境に含まれている異なる顧客の仮想クラウドネットワーク間で共有されているハブＶＮＥＴ１１２２を含み、すなわち、ハブＶＮＥＴ１１２２は、第１のクラウド環境１１３５のリージョンに含まれている複数の顧客のＶＣＮのトラフィックを処理する。図１１に示されているように、第２のクラウド環境１１０５のリージョンは、高帯域幅ネットワーク相互接続１１１５によって、第１のクラウド環境１１３５のリージョンに通信可能に接続される。以下では、（第２のクラウド環境１１０５のリージョンに含まれている）顧客１のＶＮＥＴ１１０１と（第１のクラウド環境１

１３５のリージョンに含まれている）顧客１のＶＣＮ１１３１の間のエンドツーエンドのネットワーク経路を構成することについての詳細な説明が提供されている。

【０１７８】

図１１に示されているように、顧客１のＶＮＥＴ１１０１内で実行される（例えば、ユーザ１１０１Ａによって操作される）仮想マシンからトラフィックを受信するために、第１のリンク有効化仮想ネットワーク１１０３（すなわち、リーフ１ＶＮＥＴ）が、顧客１のＶＮＥＴ１１０１にピアリングされる。ハブＶＮＥＴ１１１０が第２のクラウド環境１１０５のリージョン内の複数の顧客のＶＮＥＴ間で共有されるため、本開示の一部の実装では、第２のクラウド環境１１０５のリージョン内の顧客のＶＮＥＴから生じる異なる顧客のトラフィックを区別するために、カプセル化およびトンネルフレームワークが利用される。第１のリンク有効化仮想ネットワーク１１０３は、ネットワークアダプタ１１０３Ａ（本明細書では、リモート仮想ネットワークアダプタ（ＲＶＮＡ：remote virtual network adaptors）と呼ばれる）の対を含む。第１のリンク有効化仮想ネットワーク１１０３に含まれているネットワークアダプタ１１０３Ａの各々は、顧客１のＶＮＥＴ１１０１から受信されたトラフィックをカプセル化して、カプセル化されたトラフィックを生成するように構成される。

【０１７９】

一部の実装では、ネットワークアダプタ１１０３Ａの対は、高可用性を実現する目的で使用され、アクティブ－アクティブ状態に維持される。言い換えると、ネットワークアダプタ１１０３Ａの対に含まれている各アダプタは、機能的であり、顧客１のＶＮＥＴ１１０１から受信されたトラフィックをカプセル化する。一部の実施形態では、ネットワークアダプタ１１０３Ａの対は、ＢＧＰピアリングを実行する目的で、第２のクラウド環境１１０５によって提供されたサービスを利用してよい。ネットワークアダプタ１１０３Ａの対は、そのようなサービスに、等コストマルチパスルーティング（ＥＣＭＰ：equal cost multi-path routing）などのメカニズムを使用することによって、均一な方法で（顧客のＶＮＥＴから生じる）トラフィックを分散するように指示してよい。例えば、第２のクラウド環境１１０５がAzureクラウド（すなわち、Microsoftによって運用されているクラウド）に対応するということを考慮して、ネットワークアダプタ１１０３Ａの対は、ＢＧＰピアリングを実行する目的で、Azureルートサーバ（ＡＲＳ：Azure route server）を利用してよい。

【０１８０】

しかし、第２のクラウド環境のそのようなサービス（例えば、ＡＲＳ）の利用は、いくつかの制限を課す。例えば、ＡＲＳなどのサービスは、直接ピアリングされたＶＮＥＴ内のルートのみを学習して伝搬することができる。これは、サービスがＲＶＮＡルートを顧客のＶＮＥＴに投入するために、（第２のクラウド環境によって提供された）サービスが、第１のリンク有効化仮想ネットワーク（すなわち、リーフＶＮＥＴ１１０３）に存在するか、または顧客のＶＮＥＴ１１０１と直接ピアリングされている分離したＶＮＥＴに存在する必要があるということを意味する。２つのＶＮＥＴのピアを顧客のネットワークに含めることによる顧客の混乱を防ぐために、本開示の１つの実施形態によって、サービス（例えば、ＡＲＳ）が第１のリンク有効化仮想ネットワーク１１０３に配置されるのが好ましい。

【０１８１】

一部の実施形態によれば、第２のクラウド環境のある種の制限は、ピアリングにおける両方のＶＮＥＴが、その内部にデプロイされた仮想ネットワークゲートウェイ（ＶＮＧ：virtual network gateway）またはサービス（例えば、ＡＲＳ）のいずれかを含む場合に、ＶＮＥＴを経由するルート伝搬を禁止することである。ハブＶＮＥＴ１１１０がＶＮＧ１１１２を含み、第１のリンク有効化仮想ネットワーク１１０３がサービス（例えば、ＡＲＳ）をホストするため、これらの２つのＶＮＥＴを直接ピアリングすることは、ＶＮＧに次にホップされるハブＶＣＮ１１２２のＣＩＤＲのルートが自動的に設置されず、ユーザ定義ルート（ＵＤＲ：user defined routes）によって構成可能でもないという

ことを意味する。そのため、ネットワークインダイレクションの追加のレイヤが、第１のリンク有効化仮想ネットワーク１１０３とハブＶＮＥＴ１１１０の間に導入される。詳細には、図１１に示されているように、トラフィックを第１のリンク有効化仮想ネットワーク１１０３からハブＶＮＥＴ１１１０に転送するために、第２のリンク有効化仮想ネットワーク１１０７がネクストホップとして導入される。

【０１８２】

第２のリンク有効化仮想ネットワーク１１０７は、仮想ネットワークフォワーダ（ＶＮＦ：virtual network forwarder）の対１１０７Ａを含む。ＶＮＦの対１１０７Ａに含まれている各ＶＮＦは、第１のリンク有効化仮想ネットワーク１１０３から受信された、カプセル化されたトラフィックを、第２のクラウド環境１１０５のリージョンに含まれているハブ仮想ネットワーク１１１０に転送するように構成される。一部の実装では、仮想ネットワークフォワーダ（ＶＮＦ）の対１１０７Ａは、第１のリンク有効化仮想ネットワーク１１０３から受信されているカプセル化されたトラフィックに対して、ネットワークアドレス変換（ＮＡＴ）を実行する。詳細には、仮想ネットワークフォワーダ（ＶＮＦ）の対１１０７Ａは、データパケットが仮想ネットワークインターフェイスカード（ＶＮＩＣ）、例えば、第１のクラウド環境１１３５のリージョンのハブＶＣＮ１１２２に含まれているＶＮＩＣ１１２２Ａに送信されるように、第１のリンク有効化仮想ネットワーク１１０３から受信されている各データパケットに対してＮＡＴ動作を実行する。仮想ネットワークフォワーダ（ＶＮＦ）の対１１０７Ａが、トラフィックをハブＶＮＥＴ１１１０に含まれているＶＮＧ１１１２に転送し、その後、トラフィックが、高帯域幅相互接続１１１５を介して（第１のクラウド環境１１３５のリージョンに含まれている）ハブＶＣＮ１１２２に伝達されるということが理解される。

【０１８３】

一部の実施形態によれば、ハブＶＣＮ１１２２に含まれているＶＮＩＣ（例えば、ＶＮＩＣ１１２２Ａ）によって受信された、カプセル化されたトラフィックが、第１のクラウド環境１１３５のリージョンに含まれている第３のリンク有効化仮想ネットワーク１１２３（スポークＶＣＮとしてラベル付けされている）に転送される。第３のリンク有効化仮想ネットワーク１１２３は、仮想ネットワークアダプタの対１１２３Ａ（ローカル仮想ネットワークアダプタ（ＬＶＮＡ：local virtual network adaptors）としてラベル付けされている）を含み、これらの仮想ネットワークアダプタの各々は、ハブＶＣＮ１１２２に含まれているＶＮＩＣ１１２２Ａから受信された、カプセル化されたトラフィックをカプセル解除するように構成される。さらに、図１１に示されているように、第１のクラウド環境１１３５の第３のリンク有効化仮想ネットワーク１１２３に含まれている仮想ネットワークアダプタの対１１２３Ａは、カプセル解除されたトラフィックを、ダイナミックルーティングゲートウェイ（ＤＲＧ）接続を介して顧客１のＶＣＮ１１３１に（例えば、顧客１のＶＣＮ１１３１にデプロイされているリソース１１３１Ａに）送信する。

【０１８４】

このようにして、第１のリンク有効化仮想ネットワーク１１０３、第２のリンク有効化仮想ネットワーク１１０７、（第１のクラウド環境内の）ハブＶＮＥＴ１１１０、（第２のクラウド環境内の）ハブＶＣＮ１１２２、および第３のリンク有効化仮想ネットワーク１１２３を介して、第２のクラウド環境１１０５のリージョン内の顧客１のＶＮＥＴ１１０１と、第１のクラウド環境１１３５のリージョン内の顧客１のＶＣＮ１１３１の間に、エンドツーエンドのネットワークリンクが確立される。顧客１のＶＮＥＴと顧客１のＶＣＮの間に確立されるネットワークリンクに関して上で説明された方法と同様の方法で、（第２のクラウド環境１１０５のリージョン内の）顧客２のＶＮＥＴ１１０２と、（第１のクラウド環境１１３５のリージョン内の）顧客２のＶＣＮ１１３２の間に、ネットワークリンクが確立され得るということが理解される。さらに、第１のクラウド環境および第２のクラウド環境内の顧客の仮想ネットワークは、ＩＰアドレス空間を共有してよいが、トラフィックの衝突を防ぐために、第１のクラウド環境および第２のクラウド環境に含まれている第１のリンク有効化仮想ネットワーク、第２のリンク有効化仮想ネットワーク、第

３のリンク有効化仮想ネットワーク、およびハブ仮想ネットワークの各々に、固有のクラスレスドメイン間ルーティングＩＰアドレス空間が割り当てられるということに注意する。

【０１８５】

図１２Ａおよび図１２Ｂは、ある実施形態による、図１１のネットワークリンクのアーキテクチャに関して観察された例示的な待ち時間値を示している。詳細には、図１１を参照して上で説明されたネットワークリンクのアーキテクチャは、３ミリ秒の待ち時間を有するように、（例えば、点線によって示されているような顧客１のＶＮＥＴと顧客１のＶＣＮの間の通信経路に対応する）観察された待ち時間をもたらす。前述の経路上の個別のコンポーネント間で観察された待ち時間の内訳が、図１２Ａに示されている。図１２Ａに示された事例では、第２のクラウド環境内でＲＶＮＡおよびＶＮＦがランダムに配置されているということに注意する。一部の実施形態によれば、（ランダムに配置されるのとは対照的に）ある条件に従ってＲＶＮＡおよびＶＮＦが配置される配置戦略を使用すると、観察される待ち時間が改善される。例えば、ＲＶＮＡおよびＶＮＦ（すなわち、顧客の仮想ネットワークに関連付けられているＲＶＮＡおよびＶＮＦ）を同じゾーン（例えば、第２のクラウド環境の可用性ゾーン）に配置すると、観察される待ち時間が改善される。例えば、個別のコンポーネント間の待ち時間の内訳を提供する図１２Ｂに示されているように、ＲＶＮＡおよびＶＮＦを第２のクラウド環境の同じ可用性ドメインに配置することによって、エンドツーエンドの待ち時間が３ミリ秒から１．６ミリ秒に減らされることが観察される。

【０１８６】

図１２Ｃは、ある実施形態による、ネットワークリンクを確立するプロセスを示す例示的なフローチャートを示している。図１２Ｃに示された処理は、それぞれのシステムの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）、ハードウェア、またはこれらの組合せにおいて実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。図１２Ｃに提示され、下で説明される方法は、例示的かつ非限定的であるよう意図されている。図１２Ｃは、特定のシーケンスまたは順序で発生するさまざまな処理ステップを示しているが、これは、限定することを意図されていない。ある代替の実施形態では、これらのステップは、何らかの異なる順序で実行されてよく、または一部のステップは、並列に実行されてもよい。

【０１８７】

プロセスがステップ１２５０で開始し、ステップ１２５０で、第１のクラウド環境に含まれているマルチクラウドインフラストラクチャ（例えば、図７のマルチクラウドインフラストラクチャ７２０Ｂ）が、第１のクラウド環境内の第１の仮想ネットワーク（例えば、図１１の顧客１のＶＣＮ１１３１）と第２のクラウド環境内の第２の仮想ネットワーク（例えば、図１１の顧客１のＶＮＥＴ１１０１）の間にネットワークリンクを作成する要求を受信する。第２のクラウド環境１１０５内の顧客のテナンシに関連付けられたユーザが、第１のクラウド環境１１３５内で提供された１つまたは複数のサービスにアクセスできるようにするために、第１のクラウド環境内の第１の仮想ネットワークがすでに作成されているということに注意する。その後、プロセスが、第１の仮想ネットワークと第２の仮想ネットワークの間にネットワークリンクを作成するために、ステップ１２６０に進む。

【０１８８】

ステップ１２６０で、ネットワークリンクを作成するプロセスは、第２のクラウド環境内の第１のリンク有効化仮想ネットワークによって、第２の仮想ネットワークから受信されているトラフィックをカプセル化して、カプセル化されたトラフィックを生成することを含む。例えば、図１１を参照すると、ＲＶＮＡを含んでいる第１のリンク有効化仮想ネットワーク１１０３が、顧客１のＶＮＥＴ１１０１から受信されたトラフィックをカプセル化する（ステップ１２６３）。

【０１８９】
さらに、ステップ１２６５で、第２のクラウド環境内の第２のリンク有効化仮想ネットワーク（例えば、図１１のリンク有効化仮想ネットワーク１１０７）が、第１のリンク有効化仮想ネットワークから受信された、カプセル化されたトラフィックを、（例えば、ＶＮＦによって）第２のクラウド環境に含まれているハブ仮想ネットワーク（例えば、ハブＶＮＥＴ１１１０）に転送する。次に、プロセスがステップ１２６７に移動し、ステップ１２６７で、第１のクラウド環境内の第３のリンク有効化仮想ネットワーク（例えば、図１１のリンク有効化仮想ネットワーク１１２３）が、ハブ仮想ネットワーク、例えば、ハブＶＣＮ１１２２から受信された、カプセル化されたトラフィックを（例えば、ＬＶＮＡによって）カプセル解除する。さらに、ステップ１２６９で、第１のクラウド環境内の第３のリンク有効化仮想ネットワークが、カプセル解除されたトラフィックを、ＤＲＧ接続を介して第１のクラウド環境内の第１の仮想ネットワーク（例えば、図１１の顧客１のＶＣＮ１１３１）に送信する。このようにして、本開示のマルチクラウドインフラストラクチャは、異なる顧客の仮想ネットワーク間で、高性能で高可用性の、待ち時間の短いネットワークリンクを構成する。

【０１９０】
図１３を参照すると、ある実施形態による、ネットワークリンク構成の詳細なアーキテクチャ１３００が示されている。図１３に示されているように、ネットワークリンクが、第２のクラウド環境１３０５のリージョンを第１のクラウド環境１３３５のリージョンに通信可能に結合する。第２のクラウド環境１３０５のリージョンは、１つまたは複数の顧客のＶＮＥＴを含んでよい。例えば、第２のクラウド環境１３０５のリージョンは、２つの顧客のＶＮＥＴ、すなわち、顧客１のＶＮＥＴ１３０１および顧客２のＶＮＥＴ１３０２を含む。したがって、顧客のＶＮＥＴをホストしている第２のクラウド環境１３０５の一部は、顧客ドメイン１３５０Ａとして表される。同様に、第１のクラウド環境１３３５のリージョンは、１つまたは複数の顧客のＶＣＮ（すなわち、顧客の仮想ネットワーク）を含んでよい。例えば、第１のクラウド環境１３３５のリージョンは、２つの顧客のＶＣＮ、すなわち、顧客１のＶＣＮ１３３１および顧客２のＶＣＮ１３３２を含む。したがって、顧客のＶＣＮをホストしている第１のクラウド環境１３３５の一部は、顧客ドメイン１３５０Ｃとして表される。

【０１９１】
一部の実施形態によれば、マルチクラウドネットワークインフラストラクチャ（ＭＣＮＩ）ドメイン１３５０Ｂ、すなわち、ネットワークリンクは、顧客の仮想ネットワークの対を通信可能に結合する。例えば、図１３に示されているように、（第２のクラウド環境１３０５のリージョンに含まれている）顧客１のＶＮＥＴ１３０１は、（第１のクラウド環境１３３５のリージョンに含まれている）顧客１のＶＣＮ１３３１と通信可能に結合される。同様の方法で、（第２のクラウド環境１３０５のリージョンに含まれている）顧客２のＶＮＥＴ１３０２は、（第１のクラウド環境１３３５のリージョンに含まれている）顧客２のＶＣＮ１３３２と通信可能に結合される。ＭＣＮＩドメイン１３５０がネットワークリンクドメインに対応し、点線１３６０と１３７０の間に配置されるということに注意する。より詳細には、ＭＣＮＩドメインは、第２のクラウド環境１３０５のリージョンに配置されている第１の部分、および第１のクラウド環境１３３５のリージョンに配置されている第２の部分を含む。

【０１９２】
一部の実装では、顧客の仮想ネットワーク（例えば、第２のクラウド環境１３０５のリージョン内の顧客１のＶＮＥＴ１３０１および第１のクラウド環境１３３５のリージョン内の顧客１のＶＣＮ１３３１）の各対が、マルチクラウドネットワーク（ＭＣＮ）サービスによって（第１のクラウド環境および第２のクラウド環境に）デプロイされている複数の仮想ネットワーク（本明細書では、リンク有効化仮想ネットワークと呼ばれる）を使用して通信可能に結合される。例えば、第１のリンク有効化仮想ネットワーク１３０３（リーフ１ＶＮＥＴとしてラベル付けされている）が、第２のクラウド環境１３０５のリージ

ョンにデプロイされる。第２のリンク有効化仮想ネットワーク１３２３（スポーク１ＶＣＮとしてラベル付けされている）が、第１のクラウド環境１３３５のリージョンにデプロイされる。同様の方法で、顧客２のＶＮＥＴ１３０２が、第２のクラウド環境１３０５のリージョンおよび第１のクラウド環境１３３５のリージョンにそれぞれデプロイされているリンク有効化仮想ネットワーク１３０４（リーフ２ＶＮＥＴとしてラベル付けされている）および別のリンク有効化仮想ネットワーク１３２４（スポーク２ＶＣＮとしてラベル付けされている）に関連付けられる。したがって、図１３のアーキテクチャでは、顧客の仮想ネットワークの各対が、２つのリンク有効化仮想ネットワークに関連付けられる。

【０１９３】

さらに、第２のクラウド環境１３０５のリージョンは、第２のクラウド環境に含まれている異なる顧客の仮想ネットワーク間で共有されているハブＶＮＥＴ１３１０を含む。言い換えると、ハブＶＮＥＴ１３１０は、第２のクラウド環境１３０５のリージョンに含まれている複数の顧客のテナンシのトラフィックを処理する。同様に、第１のクラウド環境１３３５のリージョンは、第１のクラウド環境に含まれている異なる顧客の仮想クラウドネットワーク間で共有されているハブＶＣＮ１３２２を含み、すなわち、ハブＶＣＮ１３２２は、第１のクラウド環境１３３５のリージョンに含まれている複数の顧客のＶＣＮのトラフィックを処理する。図１３に示されているように、第２のクラウド環境１３０５のリージョンは、高帯域幅ネットワーク相互接続１３１５によって、第１のクラウド環境１３３５のリージョンに通信可能に接続される。以下では、（第２のクラウド環境１３０５のリージョンに含まれている）顧客１のＶＮＥＴ１３０１と（第１のクラウド環境１３３５のリージョンに含まれている）顧客１のＶＣＮ１３３１の間のエンドツーエンドのネットワーク経路を構成することについての詳細な説明が提供されている。

【０１９４】

図１３に示されているように、顧客１のＶＮＥＴ１３０１内で操作される（例えば、ユーザ１３０１Ａによって操作される）仮想マシンからトラフィックを受信するために、第１のリンク有効化仮想ネットワーク１３０３（すなわち、リーフ１ＶＮＥＴ）が、顧客１のＶＮＥＴ１３０１にピアリングされる。ハブＶＮＥＴ１３１０が第２のクラウド環境１３０５のリージョン内の複数の顧客のＶＮＥＴ間で共有されるため、本開示の一部の実装では、第２のクラウド環境１３０５のリージョン内の顧客のＶＮＥＴから生じる異なる顧客のトラフィックを区別するために、カプセル化およびトンネルフレームワークが利用される。第１のリンク有効化仮想ネットワーク１３０３は、ネットワークアダプタ１３０３Ａ（本明細書では、リモート仮想ネットワークアダプタ（ＲＶＮＡ）と呼ばれる）の対を含む。第１のリンク有効化仮想ネットワーク１３０３に含まれているネットワークアダプタ１３０３Ａの各々は、顧客１のＶＮＥＴ１３０１から受信されたトラフィックをカプセル化して、カプセル化されたトラフィックを生成するように構成される。

【０１９５】

一部の実装では、ネットワークアダプタ１３０３Ａの対は、高可用性を実現する目的で使用され、アクティブ－アクティブ状態に維持される。言い換えると、ネットワークアダプタ１３０３Ａの対に含まれている各アダプタは、機能的であり、顧客１のＶＮＥＴ１３０１から受信されたトラフィックをカプセル化する。一部の実施形態では、ネットワークアダプタ１３０３Ａの対は、ＢＧＰピアリングを実行する目的で、第２のクラウド環境１３０５によって提供されたサービスを利用してよい。ネットワークアダプタ１３０３Ａの対は、そのようなサービスに、等コストマルチパスルーティング（ＥＣＭＰ）などのメカニズムを使用することによって、均一な方法で（顧客のＶＮＥＴから生じる）トラフィックを分散するように指示してよい。

【０１９６】

図１３に示されているように、ハブＶＮＥＴ１３１０は、仮想ネットワークフォワーダ（ＶＮＦ）１３０６および１３０７の対を含む。ＶＮＦの対は、第２のクラウド環境１３０５のリージョンに含まれている顧客のＶＮＥＴごとに関連付けられる。例えば、ＶＮＦの対１３０７が顧客１のＶＮＥＴ１３０１に関連付けられ、ＶＮＦの対１３０６が顧客２

のＶＮＥＴ１３０１に関連付けられる。ＶＮＦの対１３０７に含まれている各ＶＮＦは、第１のリンク有効化仮想ネットワーク１３０３から（すなわち、対応するＲＶＮＡから）受信された、カプセル化されたトラフィックを、第１のクラウド環境１３３５のリージョンに含まれているハブ仮想ネットワーク１３２２に転送するように構成される。

【０１９７】

一部の実装では、仮想ネットワークフォワーダ（ＶＮＦ）の対１３０７は、第１のリンク有効化仮想ネットワーク１３０３から受信されているカプセル化されたトラフィックに対して、ネットワークアドレス変換（ＮＡＴ）を実行する。詳細には、仮想ネットワークフォワーダ（ＶＮＦ）の対１３０７は、データパケットが仮想ネットワークインターフェイスカード（ＶＮＩＣ）、例えば、第１のクラウド環境１３３５のリージョンのハブＶＣＮ１３２２に含まれているＶＮＩＣ１３２２Ａに送信されるように、第１のリンク有効化仮想ネットワーク１３０３から受信されている各データパケットに対してＮＡＴ動作を実行する。仮想ネットワークフォワーダ（ＶＮＦ）の対１３０７が、トラフィックをハブＶＮＥＴ１３１０に含まれている仮想ネットワークゲートウェイ（ＶＮＧ）１３１２に転送し、その後、トラフィックが、高帯域幅相互接続１３１５を介して（第１のクラウド環境１３３５のリージョンに含まれている）ハブＶＣＮ１３２２に伝達されるということが理解される。

【０１９８】

一部の実施形態によれば、ハブＶＣＮ１３２２に含まれているＶＮＩＣ（例えば、ＶＮＩＣ１３２２Ａ）によって受信された、カプセル化されたトラフィックが、第１のクラウド環境１３３５のリージョンに含まれている第２のリンク有効化仮想ネットワーク１３２３（スポークＶＣＮとしてラベル付けされている）に転送される。第２のリンク有効化仮想ネットワーク１３２３は、仮想ネットワークアダプタの対１３２３Ａ（ローカル仮想ネットワークアダプタ（ＬＶＮＡ）としてラベル付けされている）を含み、これらの仮想ネットワークアダプタの各々は、ハブＶＣＮ１３２２に含まれているＶＮＩＣ１３２２Ａから受信された、カプセル化されたトラフィックをカプセル解除するように構成される。さらに、図１３に示されているように、第１のクラウド環境１３３５の第２のリンク有効化仮想ネットワーク１３２３に含まれている仮想ネットワークアダプタの対１３２３Ａは、カプセル解除されたトラフィックを、ダイナミックルーティングゲートウェイ（ＤＲＧ）接続を介して顧客１のＶＣＮ１３３１に（例えば、顧客１のＶＣＮ１３３１にデプロイされているリソース１３３１Ａに）送信する。

【０１９９】

このようにして、第１のリンク有効化仮想ネットワーク１３０３、第２のリンク有効化仮想ネットワーク１３２３、（第１のクラウド環境内の）ハブＶＮＥＴ１３１０、および（第２のクラウド環境内の）ハブＶＣＮ１３２２を介して、第２のクラウド環境１３０５のリージョン内の顧客１のＶＮＥＴ１３０１と、第１のクラウド環境１３３５のリージョン内の顧客１のＶＣＮ１３３１の間に、エンドツーエンドのネットワークリンクが確立される。顧客１のＶＮＥＴと顧客１のＶＣＮの間に確立されるネットワークリンクに関して上で説明された方法と同様の方法で、（第２のクラウド環境１３０５のリージョン内の）顧客２のＶＮＥＴ１３０２と、（第１のクラウド環境１３３５のリージョン内の）顧客２のＶＣＮ１３３２の間に、ネットワークリンクが確立され得るということが理解される。さらに、第１のクラウド環境および第２のクラウド環境内の顧客の仮想ネットワークは、ＩＰアドレス空間を共有して（例えば、重複するＩＰアドレス空間を有して）よいが、トラフィックの衝突を防ぐために、第１のクラウド環境および第２のクラウド環境に含まれている第１のリンク有効化仮想ネットワーク、第２のリンク有効化仮想ネットワーク、およびハブ仮想ネットワークの各々に、固有のクラスレスドメイン間ルーティングＩＰアドレス空間が割り当てられるということに注意する。

【０２００】

図１４Ａは、一部の実施形態による、図１３の相互接続共有構造の例示的な観察された待ち時間の内訳を示している。この構成では、（顧客１のＶＮＥＴから顧客１のＶＣＮへ

の例示的な経路１の）エンドツーエンドの待ち時間が９５０マイクロ秒であることが観察される。したがって、本開示は、パケットプロセッサの戦略的配置を提供し、例えば、ＶＮＦがハブＶＮＥＴに配置され、エクサデータベースアプリケーションなどの、ハイスループットの待ち時間に敏感なアプリケーションをサポートすることにとって有利な、短い待ち時間を実現する。前述の実施形態では、待ち時間測定結果が、顧客のＶＮＥＴおよび顧客のＶＣＮの、すなわち、可用性ゾーンおよびリージョン内の、特定の設定に対応するということに注意する。

【０２０１】

図１４Ｂは、ある実施形態による、ネットワークリンクを確立するプロセスを示す別の例示的なフローチャートを示している。図１４Ｂに示された処理は、それぞれのシステムの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）、ハードウェア、またはこれらの組合せにおいて実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。図１４Ｂに提示され、下で説明される方法は、例示的かつ非限定的であるよう意図されている。図１４Ｂは、特定のシーケンスまたは順序で発生するさまざまな処理ステップを示しているが、これは、限定することを意図されていない。ある代替の実施形態では、これらのステップは、何らかの異なる順序で実行されてよく、または一部のステップは、並列に実行されてもよい。

【０２０２】

プロセスがステップ１４５０で開始し、ステップ１４５０で、第１のクラウド環境に含まれているマルチクラウドインフラストラクチャ（例えば、図７のマルチクラウドインフラストラクチャ７２０Ｂ）が、第１のクラウド環境内の第１の仮想ネットワーク（例えば、図１３の顧客１のＶＣＮ１３３１）と第２のクラウド環境内の第２の仮想ネットワーク（例えば、図１３の顧客１のＶＮＥＴ１３０１）の間にネットワークリンクを作成する要求を受信する。第２のクラウド環境１３０５内の顧客のテナンシに関連付けられたユーザが、第１のクラウド環境１３３５内で提供された１つまたは複数のサービスにアクセスできるようにするために、第１のクラウド環境内の第１の仮想ネットワークがすでに作成されているということに注意する。その後、プロセスが、複数のリンク有効化仮想ネットワークを使用して第１の仮想ネットワークと第２の仮想ネットワークの間にネットワークリンクを作成するために、ステップ１４５５に進む。

【０２０３】

次に、プロセスがステップ１４６０に移動し、ステップ１４６０で、複数のリンク有効化仮想ネットワークからの第１のリンク有効化仮想ネットワークが、第２のクラウド環境に配置される。例えば、図１３を参照すると、第１のリンク有効化仮想ネットワーク１３０３が、顧客のＶＮＥＴとピアリングするために、第２のクラウド環境のリージョンにデプロイされる。プロセスが、ステップ１４６５で、複数のリンク有効化仮想ネットワークからの第２のリンク有効化仮想ネットワークを第１のクラウド環境に配置／デプロイする。例えば、図１３を参照すると、第２のリンク有効化仮想ネットワーク１３２３が、ＤＲＧ接続を介して顧客のＶＣＮとピアリングするために、第１のクラウド環境のリージョンにデプロイされる。このようにして、本開示のマルチクラウドインフラストラクチャは、異なる顧客の仮想ネットワーク間で、高性能で高可用性の、待ち時間の短いネットワークリンクを構成する。

【０２０４】

図１５は、ある実施形態による、マルチクラウドネットワークサービス制御プレーン（ＭＣＮＳ－ＣＰ：multi-cloud network service control plane）を含んでいるサービスインフラストラクチャ１５００のアーキテクチャを示している。ＭＣＮＳ－ＣＰは、図１１および図１３を参照して上で説明されたネットワークリンクのようなネットワークリンクを構成する役割を担う。図１５に示されているように、サービスアーキテクチャ１５００は、高帯域幅相互接続（例えば、Express RouteまたはFast Connect）を介して互いに通信可能に結合され得る第２のクラウド環境１５０１のリージョンおよび第１

のクラウド環境１５５１のリージョンを含んでいる。第２のクラウド環境１５０１のリージョンは、顧客のＶＮＥＴ１５０３、スポークＶＮＥＴ１５０５、リーフＶＮＥＴ１５０７、ハブＶＮＥＴ１５０９、およびマルチクラウドサービスＶＮＥＴ１５１０を含む。顧客のＶＮＥＴ１５０３は顧客ドメインに対応し、一方、スポークＶＮＥＴ１５０５およびリーフＶＮＥＴ１５０７は、顧客ごとにインスタンス化されるサービスドメインに対応する。ハブＶＮＥＴ１５０９およびマルチクラウドサービスＶＮＥＴ１５１０が、マルチテナントされているサービスプレーンの一部に対応するということが理解される。

【０２０５】

リーフＶＮＥＴ１５０７は、顧客のＶＮＥＴ１５０３とピアリングし、顧客のＶＮＥＴ１５０３との間で受信されたトラフィックをカプセル化／カプセル解除するように構成されている１つまたは複数の仮想ネットワークアダプタ（例えば、ＲＶＮＡ１５０７Ａ）を含む。スポークＶＮＥＴ１５０５は、リーフＶＮＥＴ１５０７から受信されたトラフィックをハブＶＮＥＴ１５０９に転送するように構成されている１つまたは複数の仮想ネットワークフォワーダ（例えば、ＶＮＦ１５０５Ａ）を含む。さらに、リーフＶＮＥＴ１５０７およびスポークＶＮＥＴ１５０５の各々はプライベートエンドポイントを含み、プライベートエンドポイントを介して、ネットワーク構成情報がＲＶＮＡおよびＶＮＦにそれぞれ提供されてよい。例えば、リーフＶＮＥＴ１５０７はプライベートエンドポイント１５０７Ｂを含み、スポークＶＮＥＴ１５０５はプライベートエンドポイント１５０５Ｂを含み、これらのプライベートエンドポイントを介して、ネットワーク構成情報（すなわち、マッピング情報）が取得され得る。以下では、ネットワーク構成情報の配布に関する詳細がさらに説明される。

【０２０６】

ハブＶＮＥＴ１５０９は、第２のクラウド環境を第１のクラウド環境に結合するために、高帯域幅相互接続に通信可能に結合されている仮想ネットワークゲートウェイ（ＶＮＧ）を含む。一部の実装では、ハブＶＮＥＴ１５０９は、仮想ネットワーク内でプロビジョニングされている、完全にプラットフォームによって管理されたＰａａＳサービスであるBastion１５０９Ａを含んでよい。特に、Bastion１５０９は、例えば、ブラウザを使用する、ネイティブＳＳＨを介する、などによって、仮想マシンに接続することを可能にするサービスである。マルチクラウドサービスＶＮＥＴ１５１０は、内部ロードバランサ（ＩＬＢ：load balancer）１５１０Ｂおよびアウトポスト１５１０Ａを含む。アウトポスト１５１０ＡとＩＬＢ１５１０Ｂの組合せは、（第１のクラウド環境から受信された）ネットワーク構成情報をプライベートエンドポイント１５０５Ｂおよび１５０７Ｂに配布するために使用される。このようにして、ＶＮＦ１５０５ＡおよびＲＶＮＡ１５０７Ａは、それぞれのプライベートエンドポイント、すなわち、プライベートエンドポイント１５０５Ｂおよびプライベートエンドポイント１５０７Ｂから、ネットワーク構成情報を受信することができる。

【０２０７】

第１のクラウド環境１５５１のリージョンは、リソース１５５８（例えば、エクサデータベース）をホストする顧客のＶＣＮ１５５７、スポークＶＣＮ１５５５、ハブＶＣＮ１５５３、およびマルチクラウドサービスＶＣＮ１５６０を含む。顧客のＶＣＮ１５５７は顧客ドメインに対応し、一方、スポークＶＣＮ１５５５は、顧客ごとにインスタンス化されるサービスドメインに対応する。ハブＶＣＮ１５５３およびマルチクラウドサービスＶＣＮ１５６０が、マルチテナントされているサービスプレーンの一部に対応するということが理解される。

【０２０８】

スポークＶＣＮ１５５５は、（例えば、ＤＲＧ接続を介して）顧客のＶＣＮ１５５７とピアリングし、顧客のＶＣＮ１５５７との間で受信されたトラフィックをカプセル化／カプセル解除するように構成されている１つまたは複数の仮想ネットワークアダプタ（例えば、ＬＶＮＡ１５５５Ａ）を含む。スポークＶＣＮ１５５５は、ＶＮＩＣ接続を含み、ＶＮＩＣ接続を介してマルチクラウドサービスＶＣＮ１５６０と通信する。例えば、スポー

クＶＣＮ１５５５に含まれているＬＶＮＡ１５５５Ａは、ネットワーク構成情報を受信するために、マルチクラウドサービスＶＣＮ１５６０に含まれているＶＮＩＣに接続する。スポークＶＣＮ１５５５は、ハブＶＣＮ１５５３に含まれている別のＶＮＩＣ接続１５５３Ｂを介して、ハブＶＣＮ１５５３にさらに通信可能に結合される。ハブＶＣＮ１５５３はＤＲＧを含み、ＤＲＧを介して、ハブＶＣＮ１５５３が、第１のクラウド環境を第２のクラウド環境に結合する高帯域幅相互接続に結合される。

【０２０９】

一部の実施形態によれば、マルチクラウドサービスＶＣＮ１５６０は、第１のクラウド環境１５５１内に構築されている制御プレーンのスタックに対応する。詳細には、マルチクラウドサービスは、ＶＣＮ、ルートテーブル、ＤＲＧ、接続、ＶＮＥＴ、インスタンス、ＶＮＩＣ、ピアリングなどの、複数のネットワークリソースで構成される。マルチクラウドサービスＶＣＮ１５６０は、ロードバランサ１５６０Ａ、１つまたは複数のＡＰＩサーバ１５６０Ｂ、キー値ストア１５６０（Ｋ－Ｖストアとしてラベル付けされている）、配布サービス１５６０Ｄ、ＷＦａａＳ（workflow-as-a-service）ワーカー１５６０Ｆ、およびゲートウェイ１５６０Ｇを含む。一部の実装では、１つまたは複数のＡＰＩサーバ１５６０Ｂは、第１のクラウド環境と第２のクラウド環境の間のネットワークリンクを設定する要求を受信する。それに応じて、１つまたは複数のＡＰＩサーバ１５６０Ｂは、（ＷＦａａＳワーカー１５６０Ｆに含まれている）ワーカーを開始してよい。一部の実装では、ＷＦａａＳワーカー１５６０は、第１のクラウド環境および第２のクラウド環境の制御プレーンとの通信を開始し、必要とされるネットワークリソースをデプロイして、ネットワークリンクをプロビジョニングし、例えば、第１のクラウド環境および第２のクラウド環境内のリンク有効化仮想ネットワークを起動し、ネットワークリンク接続をピアリングする。ＷＦａａＳワーカー１５６０Ｆによって実行される１つのそのような例示的なプロセスが、図１６Ａを参照して後で説明される。１つまたは複数のＡＰＩサーバ１５６０Ｂは、マルチクラウドサービスのさまざまなコンポーネントへのＣＩＤＲアドレス割り当てを管理するように構成される。

【０２１０】

配布サービス１５６０Ｄは、ＲＶＮＡ、ＶＮＦ、およびＬＶＮＡから要求（例えば、マッピング要求）を受信するマッピングサービスである。配布サービス１５６０Ｄは、ネットワークパケット（すなわち、トラフィック）のカプセル化／カプセル解除を実行するためにＲＶＮＡ、ＶＮＦ、およびＬＶＮＡによって要求されたネットワーク構成情報を提供することによって、そのようなマッピング要求に応答する。例えば、１つの実装では、ＲＶＮＡ、ＶＮＦ、およびＬＶＮＡは、配布サービス１５６０Ｄを定期的にポーリングして、それぞれのネットワーク構成情報を取得してよい。配布サービス１５６０Ｄは、ＶＮＩＣ接続を介して、ネットワーク構成情報を（スポークＶＣＮ１５５５に位置する）ＬＶＮＡ１５５５Ａに提供する。

【０２１１】

さらに、マルチクラウドサービスＶＣＮ１５６０は、第２のクラウド環境に各々位置するＶＮＦ１５０５ＡおよびＲＶＮＡ１５０７Ａによって（それぞれのプライベートエンドポイントを介して）ネットワーク構成情報が最終的に取得され得るように、ネットワーク構成情報を（マルチクラウドサービスＶＮＥＴ１５１０に含まれている）アウトポスト１５１０Ａに送信するために、マルチクラウドサービスＶＮＥＴ１５１０との通信チャネル、例えば、トンネル（例えば、ＩＰｓｅｃトンネル）を設定してよい。特に、アウトポスト１５１０AによってＶＮＦおよびＲＶＮＡのポーリング要求が（それぞれのエンドポイント１５０５Ｂおよび１５０７Ｂを介して）受信される。次に、アウトポスト１５１０Ａが、そのような要求を配布サービス１５６０Ｄにリダイレクトする。ポーリング要求を受信することに応答して、配布サービス１５６０Ｄは、対応するネットワーク構成情報をＶＮＦおよびＲＶＮＡに提供する。一部の実装では、配布サービス１５６０Ｄは、Ｋ－Ｖストア１５６０からネットワーク構成情報を取得し、取得された情報をさまざまなパケットプロセッサ（すなわち、ＶＮＦ、ＲＶＮＡ、およびＬＶＮＡ）にさらに配布する。配布サ

ービス１５６０Ｄが、それぞれのパケットプロセッサによって発行されたポーリング要求において、ＲＶＮＡ、ＬＶＮＡ、およびＶＮＦの各々に対応する健全性の状態を示す情報を受信してよいということが理解される。さらに、マルチクラウドサービスＶＣＮ１５６０はゲートウェイ１５６０Ｇを含み、ゲートウェイ１５６０Ｇは、外部の関係者に対してマルチクラウドサービスＶＣＮ１５６０によって行われる呼び出し／要求、例えば、第２のクラウド環境に対して行われる呼び出し、パブリックＩＰアドレスに対して行われる呼び出しなどを、プロビジョニングする／可能にするために使用される。

【０２１２】

図１６Ａを参照すると、ある実施形態による、異なるクラウド環境とのマルチクラウドサービス制御プレーンの情報のやりとりを示すスイム図が示されている。図１６Ａのスイム図は、クライアント１６０１、マルチクラウドプラットフォーム制御プレーン１６０２、第２のクラウド環境のＩａａＳ　ＡＰＩ１６０３、および第１のクラウド環境１６０４に対応するＩａａＳ　ＡＰＩという実体の間の情報のやりとりを示している。

【０２１３】

図１６Ａに示されているように、ステップＳ１で、ネットワークリンクを作成するためにクライアント１６０１によって発行された要求が、マルチクラウドプラットフォーム制御プレーン１６０２によって受信される。一部の実装では、マルチクラウドプラットフォーム制御プレーン１６０２は、要求を受け取り、確認応答をクライアント１６０１に返す（ステップＳ２）。その後、クライアント１６０１が、マルチクラウドプラットフォーム制御プレーン１６０２をポーリングして、要求の状態を取得してよい。

【０２１４】

ステップＳ３で、マルチクラウドプラットフォーム制御プレーン１６０２は、ネットワークリンクを作成する要求を受け取ると、例えばＷＦａａＳワーカー（図１５の１５６０Ｆ）を使用して、ワークフローを開始する。ステップＳ４で、マルチクラウドプラットフォーム制御プレーン１６０２は、第１の要求を、第１のクラウド環境１６０４に対応するＩａａＳ　ＡＰＩに送信する。そのような要求が第１のクラウド環境の第１のエンドポイントに送信されてよいということに注意する（例えば、第１のエンドポイントは、第１のクラウド環境のリソースマネージャに対応してよい）。第１の要求は、マルチクラウドプラットフォーム制御プレーン１６０２によって発行されている要求に対応し、第１のクラウド環境内のリソースの第１のセットのプロビジョニングを要求する。リソースの第１のセットは、ＬＶＮＡ、ハブＶＣＮ、スポークＶＣＮ、ＶＮＩＣなどの作成に対応してよい。一部の実装では、第１の要求が、第１のエンドポイントに、第１のクラウド環境内のすべての必要とされるリソースの集合的インスタンス化を要求するテンプレートを含んでよいということが理解される。

【０２１５】

ステップＳ５で、マルチクラウドプラットフォーム制御プレーン１６０２は、第２の要求を、第２のクラウド環境１６０３に対応するＩａａＳ　ＡＰＩに送信する。そのような要求が第２のクラウド環境の第２のエンドポイントに送信されてよいということに注意する（例えば、第２のエンドポイントは、第２のクラウド環境のリソースマネージャに対応してよい）。第２の要求は、マルチクラウドプラットフォーム制御プレーン１６０２によって発行されている要求に対応し、第２のクラウド環境内のリソースの第２のセットのプロビジョニングを要求する。リソースの第２のセットは、ＲＶＮＡ、ＶＮＦ、ハブＶＮＥＴ、スポークＶＮＥＴ、サービスエンドポイント、ネットワークピアリングなどの作成に対応してよい。一部の実装では、第２の要求が、第２のエンドポイントに、第２のクラウド環境内のすべての必要とされるリソースの集合的インスタンス化を要求するテンプレートを含んでよいということが理解される。

【０２１６】

ステップ６および７で、マルチクラウドプラットフォーム制御プレーン１６０２が、第１のエンドポイントおよび第２のエンドポイントそれぞれから確認応答を受信してよい。その後、マルチクラウドプラットフォーム制御プレーン１６０２は、要求されたネットワ

ークリンクの状態に関するクライアント１６０１からのポーリング要求を受信すると、ステップ９で、ネットワークリンクの作成の成功を示すメッセージ（すなわち、ネットワークリンクが使用可能であることを示すメッセージ）をクライアントに送信してよい。

【０２１７】

図１６Ｂは、ある実施形態による、マルチクラウドサービス制御プレーンによって実行されるプロセスを示す例示的なフローチャートを示している。図１６Ｂに示された処理は、それぞれのシステムの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）、ハードウェア、またはこれらの組合せにおいて実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。図１６Ｂに提示され、下で説明される方法は、例示的かつ非限定的であるよう意図されている。図１６Ｂは、特定のシーケンスまたは順序で発生するさまざまな処理ステップを示しているが、これは、限定することを意図されていない。ある代替の実施形態では、これらのステップは、何らかの異なる順序で実行されてよく、または一部のステップは、並列に実行されてもよい。

【０２１８】

プロセスがステップ１６５０で開始し、ステップ１６５０で、第１のクラウド環境に含まれているマルチクラウドインフラストラクチャの制御プレーンが、第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークの間にネットワークリンクを作成する要求を受信する。第２のクラウド環境内の顧客のテナンシに関連付けられたユーザが、第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスできるようにするために、第１のクラウド環境内の第１の仮想ネットワークがすでに作成されているということに注意する。ネットワークリンクを作成する要求の受信時に、制御プレーンは、ワークフローを実行して、ネットワークリンクの作成を開始する（ステップ１６６０）。

【０２１９】

一部の実装では、ワークフローは、ネットワークリンクを作成するために実行される複数のサブステップを含んでよい。例えば、ワークフローはステップ１６６３を含んでよく、ステップ１６６３で、第１の要求が、第１のクラウド環境の第１のエンドポイントに送信される（例えば、第１のエンドポイントは、第１のクラウド環境のリソースマネージャに対応してよい）。第１の要求は、マルチクラウドプラットフォーム制御プレーン１６０２によって発行されている要求に対応し、第１のクラウド環境内のリソースの第１のセットのプロビジョニングを要求する。リソースの第１のセットは、ＬＶＮＡ、ハブＶＣＮ、スポークＶＣＮ、ＶＮＩＣなどの作成に対応してよい。

【０２２０】

その後、プロセスがステップ１６６５に移動し、ステップ１６６５で、第２の要求が、第２のクラウド環境の第２のエンドポイントに送信される（例えば、第２のエンドポイントは、第２のクラウド環境のリソースマネージャに対応してよい）。第２の要求は、マルチクラウドプラットフォーム制御プレーン１６０２によって発行されている要求に対応し、第２のクラウド環境内のリソースの第２のセットのプロビジョニングを要求する。リソースの第２のセットは、ＲＶＮＡ、ＶＮＦ、ハブＶＮＥＴ、スポークＶＮＥＴ、サービスエンドポイント、ネットワークピアリングなどの作成に対応してよい。

【０２２１】

さらに、ステップ１６７０で、リソースの第１のセットおよびリソースの第２のセットがプロビジョニングされることに応答して、制御プレーンは、ネットワーク構成情報を、リソースの第１のセットおよびリソースの第２のセットのうちの１つまたは複数のリソースに配布してよい。ネットワーク構成情報は、例えば、リソースのＩＰアドレスに対応する情報を含んでよい。そのため、パケットプロセッサに、（制御プレーンの配布サービスによって）トラフィックが転送されるネクストホップの送信先のアドレスに関する情報が提供される。言い換えると、ネットワーク構成情報は、第１のクラウド環境内の第１の仮想ネットワークと第２のクラウド環境内の第２の仮想ネットワークとの間でトラフィック

が伝達されることを可能にする。

【０２２２】

図１１および図１３に関して上で説明されたように、第１のクラウド環境と第２のクラウド環境の間に作成されるネットワークリンクのアーキテクチャは、ネットワークリンクをプロビジョニングするために作成されているリンク有効化仮想ネットワーク内のパケットプロセッサの位置および配置に関連する。本開示の実施形態によって作成されたネットワークリンクが、エクサデータベースアプリケーションなどの、ハイスループットの待ち時間に敏感なアプリケーションをサポートするということが理解される。一部の実施形態によれば、第１のクラウド環境と第２のクラウド環境の間の通信の送信待ち時間（例えば、往復待ち時間）も、計算インスタンスがプロビジョニングされる第１のクラウド環境および第２のクラウド環境内のドメインの選択による影響を受けることがある。言い換えると、短い待ち時間を実現するために、計算インスタンスをホストするドメインの最適な対（すなわち、第１のクラウド環境および第２のクラウド環境の各々に１つのドメイン）を選択するのが望ましい。

【０２２３】

クラウドインフラストラクチャが、通常はリージョンおよびドメイン（可用性ドメインとも呼ばれる）内でホストされるということに注意する。リージョンは、局所的な地理的領域として定義され、可用性ドメインは、リージョン内に位置する１つまたは複数のデータセンターに対応してよく、すなわち、リージョンは、１つまたは複数の可用性ドメインで構成される。さらに、クラウドインフラストラクチャリソースは、仮想クラウドネットワークなど、リージョンに固有であってよく、または計算インスタンスなど、可用性ドメインに固有であってよい。可用性ドメインは、互いに分離され、故障耐性があり、同時に故障する可能性が極めて低い。可用性ドメインが、電力または冷却あるいは内部の可用性ドメインネットワークなどのインフラストラクチャを共有しないため、リージョン内の１つの可用性ドメインでの故障が、同じリージョン内の他の可用性ドメインの可用性に影響を与える可能性が低い。以下では、図１７Ａを参照して、第１のクラウド環境から第２のクラウド環境へ、および第２のクラウド環境から第１のクラウド環境への情報の送信において短い待ち時間が実現されるように、計算インスタンスの配置のために第１のクラウド環境および第２のクラウド環境内の可用性ドメインを選択するためのフレームワークが説明される。

【０２２４】

図１７Ａは、ある実施形態による、異なるクラウド環境の可用性ドメイン内の計算インスタンスの例示的な配置戦略を示している。簡単にするため、および説明のために、図１７Ａは、３つの可用性ドメイン（ＡＤ）、すなわち、ＡＤ－１　１７０３Ａ、ＡＤ－２　１７０３Ｂ、およびＡＤ－３　１７０３Ｃを含んでいる第１のクラウド環境１７０１を示している。同様に、第２のクラウド環境１７２１は、３つの可用性ドメイン、すなわち、ＡＤ－１’　１７２３Ａ、ＡＤ－２’　１７２３Ｂ、およびＡＤ－３’　１７２３Ｃを含んでいるとして示されている。第２のクラウド環境内の顧客は、第１のクラウド環境によって提供されたサービス（例えば、データベースサービス）を利用することを望むことがある。第１のクラウド環境によって提供されたある種のサービス（例えば、エクサデータベースサービス）は、待ち時間に敏感であることに加えて、ハイスループットであることがある。したがって、図１７Ａに示されているように、一部の実施形態によれば、サービスをプロビジョニングするために、各クラウド環境内の特定の可用性ドメインにおける１つまたは複数の計算インスタンス１７２０のデプロイメントが必要になることがある。ＡＤがランダムな方法で顧客に割り当てられるということが、理解される。詳細には、特定のクラウド環境内の顧客１に割り当てられているＡＤ１、ＡＤ２、およびＡＤ３は、別の顧客、例えば顧客２に割り当てられている第１、第２、および第３の可用性ドメインに（順序に関して）対応しなくてよい。

【０２２５】

前述のフレームワークでは、第２のクラウド環境内の顧客が第１のクラウド環境によっ

て提供されたサービスを利用するために、望ましいサービスを可能にするように選択されたＡＤ内で１つまたは複数の計算インスタンスがデプロイされ得るように、各クラウド環境内の１つのＡＤの選択が決定されるべきである。ＡＤの対（すなわち、第１のクラウド環境内の１つのＡＤ、および第２のクラウド環境内の別のＡＤ）の選択が、選択されたＡＤによってサービスを提供することにおいて発生する待ち時間が最小になるような方法で実行されるべきであるということに注意する。ＡＤのそのような選択戦略は、待ち時間に敏感なサービスを提供することを可能にする。

【０２２６】

一部の実施形態によれば、最小の待ち時間を取得するために、各クラウド環境内のＡＤの選択が経験的に導き出される。１つの実装では、各クラウド環境内のＡＤの選択に関与するステップは、次のように説明されてよい。

ステップ１－各クラウド環境内の各可用性ドメインにおいて、単一の計算インスタンス（本明細書では、テスト計算インスタンスと呼ばれる）を割り当てる。

ステップ２－ＡＤの対（ｋ，ｊ）ごとに送信待ち時間を取得し、ｋ＝１，２，３およびｊ＝１’，２’，３’である。待ち時間が、１つのＡＤにデプロイされた計算インスタンスから他のＡＤにデプロイされた別の計算インスタンスへのデータの送信において発生する時間量に対応するということに注意する。

ステップ３－最も短い待ち時間を有するＡＤの対を選択する。

ステップ４－選択されていない（各クラウド環境内の）ＡＤ内のインスタンスをシャットダウンし、望ましい数の計算インスタンスをＡＤの選択された対の各ＡＤにデプロイする。一部の応用では、２つの計算インスタンス（すなわち、プライマリ計算インスタンスおよびセカンダリ計算インスタンス）が、各クラウド環境の選択されたＡＤにデプロイされてよい。例えば、図１７Ａに示されているように、第１のクラウド環境内のＡＤ－１　１７０３Ａおよび第２のクラウド環境内のＡＤ－２’　１７２３Ｂが、最も短い送信待ち時間をもたらすＡＤの対として決定される。そのため、サービスをプロビジョニングするために、２つの計算インスタンスがＡＤ－１　１７０３ＡおよびＡＤ－２’　１７２３Ｂの各々にデプロイされる。

【０２２７】

一部の実施形態によれば、高可用性の目的で、２つの計算インスタンスがＡＤ内の異なる障害ドメインにデプロイされてよいということに注意する。一部の他の実施形態によって、１つの計算インスタンスを最も短い待ち時間を有するＡＤの対にデプロイし、別の計算インスタンスを２番目に短い待ち時間を有する別のＡＤの対にデプロイすることを選択してよい。前述の選択戦略に基づくＡＤの他の可能な選択が、十分に本開示の範囲内であるということが、理解される。

【０２２８】

図１７Ｂは、ある実施形態による、計算インスタンスがデプロイされる異なるクラウド環境の可用性ドメインを決定することにおいてマルチクラウドサービス制御プレーンによって実行されるプロセスを示す例示的なフローチャートを示している。図１７Ｂに示された処理は、それぞれのシステムの１つまたは複数の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）、ハードウェア、またはこれらの組合せにおいて実装されてよい。ソフトウェアは、非一時的ストレージ媒体に（例えば、メモリデバイスに）格納されてよい。図１７Ｂに提示され、下で説明される方法は、例示的かつ非限定的であるよう意図されている。図１７Ｂは、特定のシーケンスまたは順序で発生するさまざまな処理ステップを示しているが、これは、限定することを意図されていない。ある代替の実施形態では、これらのステップは、何らかの異なる順序で実行されてよく、または一部のステップは、並列に実行されてもよい。

【０２２９】

プロセスがステップ１７５５で開始し、ステップ１７５５で、第１のクラウド環境に含まれているマルチクラウドインフラストラクチャが、（ｉ）第１の複数の計算インスタンスを第１のクラウド環境内の第１の複数の可用性ドメインのうちの第１の可用性ドメイン

にデプロイし、（ｉｉ）第２の複数の計算インスタンスを第２のクラウド環境内の第２の複数の可用性ドメインのうちの第２の可用性ドメインにデプロイする要求を受信する。第１のクラウド環境の第１の可用性ドメイン内の第１の複数の計算インスタンスおよび第２のクラウド環境内の第２の複数の計算インスタンスは、第２のクラウド環境内のユーザが、第１のクラウド環境内で提供された１つまたは複数のサービスにアクセスすることを可能にする。

【０２３０】

次に、プロセスがステップ１７６０に移動し、第１のクラウド環境内の第１の複数の可用性ドメインのうちの第１の可用性ドメインおよび第２のクラウド環境内の第２の複数の可用性ドメインのうちの第２の可用性ドメインを決定する。第１および第２の可用性ドメインを決定するために、プロセスがステップ１７６５に移動し、ステップ１７６５で、プロセスが、第１のクラウド環境内の第１の複数の可用性ドメインのうちの可用性ドメインごと、および第２のクラウド環境内の第２の複数の可用性ドメインのうちの可用性ドメインごとに、動作のセットを反復的に実行する。この反復的動作は、ステップ１７６５Ａ～１７６５Ｄを含む。

【０２３１】

ステップ１７６５Ａで、第１のテスト計算インスタンスが、第１のクラウド環境内の第１の複数の可用性ドメインのうちの可用性ドメインに配置される。ステップ１７６５Ｂで、第２のテスト計算インスタンスが、第２のクラウド環境内の第２の複数の可用性ドメインのうちの可用性ドメインに配置される。次に、反復プロセスがステップ１７６５Ｃに移動し、ステップ１７６５Ｃで、テストパケットが、第１のテスト計算インスタンスから第２のテスト計算インスタンスに送信される。ステップ１７６５Ｄで、第１のテスト計算インスタンスおよび第２のテスト計算インスタンスをホストしている可用性ドメインの対に対応する送信待ち時間が計算される。プロセスは、ステップ１７６５Ａ～１７６５Ｄを反復的に処理すると、ステップ１７７０に移動し、ステップ１７７０で、可用性ドメインの対に対して計算された送信待ち時間に関連付けられた条件に基づいて、第１のクラウド環境内の第１の可用性ドメインおよび第２のクラウド環境内の第２の可用性ドメインが選択される。

【０２３２】

この条件は、ステップ１７６５Ａ～１７６５Ｄの反復プロセスにおいて観察された最も短い送信待ち時間をもたらすＡＤの対を選択することに対応してよい。プロセスは、第１のクラウド環境内の第１の可用性ドメインおよび第２のクラウド環境内の第２の可用性ドメインを識別すると、選択されたドメイン内で望ましい数の計算インスタンスをインスタンス化し、第２のクラウド環境内のユーザが、第１のクラウド環境によって提供された１つまたは複数のサービスを利用できるようにしてよい。

【０２３３】

クラウドインフラストラクチャの例

前述したように、ＩａａＳ（infrastructure as a service）は、クラウドコンピューティングの１つの特定の種類である。ＩａａＳは、パブリックネットワーク（例えば、インターネット）を経由して仮想化されたコンピューティングリソースを提供するように構成され得る。ＩａａＳモデルでは、クラウドコンピューティングプロバイダは、インフラストラクチャコンポーネント（例えば、サーバ、ストレージデバイス、ネットワークノード（例えば、ハードウェア）、デプロイメントソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザレイヤ）など）をホストすることができる。場合によっては、ＩａａＳプロバイダは、それらのインフラストラクチャコンポーネントに付随して生じるように、さまざまなサービス（例えば、請求書送付、監視、ロギング、セキュリティ、ロードバランシング、およびクラスタ化など）を提供してもよい。したがって、これらのサービスはポリシー主導であることができるため、ＩａａＳユーザは、ロードバランシングを駆動してアプリケーションの可用性および性能を維持するようにポリシーを実装することができてよい。

【０２３４】
場合によっては、ＩａａＳの顧客は、インターネットなどの広域ネットワーク（ＷＡＮ）を介してリソースおよびサービスにアクセスしてよく、クラウドプロバイダのサービスを使用して、アプリケーションスタックの残りの要素をインストールすることができる。例えば、ユーザは、ＩａａＳプラットフォームにログインして、仮想マシン（ＶＭ）を作成し、オペレーティングシステム（ＯＳ）を各ＶＭにインストールし、データベースなどのミドルウェアをデプロイし、ワークロードおよびバックアップのためのストレージバケットを作成し、企業ソフトウェアをＶＭにインストールすることもできる。次に、顧客は、プロバイダのサービスを使用して、ネットワークトラフィックをバランス調整すること、アプリケーションの問題をトラブルシューティングすること、性能を監視すること、災害復旧を管理することなどを含む、さまざまな機能を実行することができる。
【０２３５】
ほとんどの場合、クラウドコンピューティングモデルは、クラウドプロバイダの参加を必要とする。クラウドプロバイダは、ＩａａＳを提供する（例えば、提供する、貸し出す、販売する）ことを専門とするサードパーティサービスであってよいが、そうである必要はない。実体は、プライベートクラウドをデプロイし、インフラストラクチャサービスのそれ自身のプロバイダになることを選択してもよい。
【０２３６】
一部の例では、ＩａａＳのデプロイメントは、新しいアプリケーションまたは新しいバージョンのアプリケーションを、準備されたアプリケーションサーバなどにつなぐプロセスである。このプロセスは、サーバを準備する（例えば、ライブラリ、デーモンなどをインストールする）プロセスを含んでもよい。このプロセスは、多くの場合、ハイパーバイザレイヤ（例えば、サーバ、ストレージ、ネットワークハードウェア、および仮想化）の下でクラウドプロバイダによって管理される。したがって、顧客は、（例えば、（例えば、オンデマンドでスピンアップされ得る）セルフサービス仮想マシンなどの上の）ＯＳ、ミドルウェア、および／またはアプリケーションのデプロイメントを処理する役割を担ってよい。
【０２３７】
一部の例では、ＩａａＳのプロビジョニングは、コンピュータまたは仮想ホストを使用のために取得すること、および必要とされるライブラリまたはサービスをそれらのコンピュータまたは仮想ホストにインストールすることも、指してよい。ほとんどの場合、デプロイメントはプロビジョニングを含まず、プロビジョニングは、最初に実行される必要があることがある。
【０２３８】
場合によっては、ＩａａＳのプロビジョニングには２つの異なる問題が存在する。第一に、何かが実行される前に、インフラストラクチャの初期セットをプロビジョニングするという最初の課題がある。第二に、すべてがプロビジョニングされた後に、既存のインフラストラクチャを発達させるという（例えば、新しいサービスを追加する、サービスを変更する、サービスを除去するなどの）課題がある。場合によっては、これらの２つの課題は、インフラストラクチャの構成が宣言的に定義されることを可能にすることによって対処されてよい。言い換えると、インフラストラクチャ（例えば、どのコンポーネントが必要とされるか、およびそれらのコンポーネントがどのように情報をやりとりするか）が、１つまたは複数の構成ファイルによって定義され得る。このようにして、インフラストラクチャのトポロジー全体（例えば、どのリソースがどのリソースに依存するか、およびそれらの各リソースがどのように連携するか）が、宣言的に記述され得る。場合によっては、トポロジーが定義された後に、構成ファイルに記述されたさまざまなコンポーネントを作成および／または管理するワークフローが生成され得る。
【０２３９】
一部の例では、インフラストラクチャは、多くの相互接続された要素を含んでよい。例えば、コアネットワークとしても知られている１つまたは複数の仮想プライベートクラウ

ド（ＶＰＣ：virtual private clouds）（例えば、構成可能な、および／または共有されたコンピューティングリソースの、場合によってはオンデマンドのプール）が存在してよい。一部の例では、ネットワークのセキュリティがどのように設定されるかを定義するためにプロビジョニングされた１つまたは複数のセキュリティグループルール、および１つまたは複数の仮想マシン（ＶＭ）が存在してもよい。ロードバランサ、データベースなどの他のインフラストラクチャ要素がプロビジョニングされてもよい。より多くのインフラストラクチャ要素が望まれ、かつ／または追加されるにつれて、インフラストラクチャが徐々に発達することができる。

【０２４０】

場合によっては、さまざまな仮想コンピューティング環境にわたってインフラストラクチャコードのデプロイメントを可能にするために、継続的デプロイメント技術が採用されてよい。さらに、説明された技術は、これらの環境内のインフラストラクチャ管理を可能にすることができる。一部の例では、サービスチームは、１つまたは複数の、ただし多くの場合は多数の、（例えば、さまざまな地理的位置にわたって、ときには世界全体にわたって）異なる実稼働環境にデプロイされるのが望ましいコードを記述する可能性がある。しかし、一部の例では、コードがデプロイされるインフラストラクチャは、最初に設定されなければならない。場合によっては、プロビジョニングが手動で行われることが可能であり、リソースをプロビジョニングするためにプロビジョニングツールが利用されてよく、かつ／またはインフラストラクチャがプロビジョニングされた後に、コードをデプロイするためにデプロイメントツールが利用されてよい。

【０２４１】

図１８は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの例示的なパターンを示すブロック図１８００である。サービスオペレータ１８０２は、仮想クラウドネットワーク（ＶＣＮ）１８０６およびセキュアホストサブネット１８０８を含むことができるセキュアホストテナンシ１８０４に通信可能に結合され得る。一部の例では、サービスオペレータ１８０２は、１つまたは複数のクライアントコンピューティングデバイスを使用していてよく、クライアントコンピューティングデバイスは、Microsoft Windows Mobile（登録商標）などのソフトウェア、および／またはiOS、Windows Phone、Android, BlackBerry 8、Palm OSなどのさまざまなモバイルオペレーティングシステムを実行している、インターネット、電子メール、ショートメッセージサービス（ＳＭＳ：short message service）、Blackberry（登録商標）、または他の通信プロトコルが有効化されている、ポータブルハンドヘルドデバイス（例えば、iPhone（登録商標）、携帯電話、iPad（登録商標）、コンピューティングタブレット、パーソナルデジタルアシスタント（ＰＤＡ：personal digital assistant））またはウェアラブルデバイス（例えば、Google Glass（登録商標）ヘッドマウントディスプレイ）であってよい。代替として、クライアントコンピューティングデバイスは、例として、Microsoft Windows（登録商標）、Apple Macintosh（登録商標）、および／またはLinux（登録商標）オペレーティングシステムのさまざまなバージョンを実行しているパーソナルコンピュータおよび／またはラップトップコンピュータを含む、汎用パーソナルコンピュータであることができる。クライアントコンピューティングデバイスは、例えばGoogle Chrome OSなどの、さまざまなGNU/Linuxオペレーティングシステムを含むが、これらに限定されない、さまざまな市販されているUNIX（登録商標）またはUNIXのようなオペレーティングシステムのいずれかを実行しているワークステーションコンピュータであることができる。代替または追加として、クライアントコンピューティングデバイスは、ＶＣＮ１８０６にアクセスできるネットワークおよび／またはインターネットを経由して通信することができる、シンクライアントコンピュータ、インターネット対応のゲーミングシステム（例えば、Kinect（登録商標）ジェスチャー入力デバイスを含むか、または含まないMicrosoft Xboxゲーム機）、および／またはパーソナルメッセージングデバイスなどの、任意の他の電子デバイスであってよい。

【０２４２】

ＶＣＮ１８０６は、ＳＳＨ　ＶＣＮ１８１２に含まれているＬＰＧ１８１０を介してセキュアシェル（ＳＳＨ）ＶＣＮ１８１２に通信可能に結合され得る、ローカルピアリングゲートウェイ（ＬＰＧ）１８１０を含むことができる。ＳＳＨ　ＶＣＮ１８１２はＳＳＨサブネット１８１４を含むことができ、ＳＳＨ　ＶＣＮ１８１２は、制御プレーンＶＣＮ１８１６に含まれているＬＰＧ１８１０を介して、制御プレーンＶＣＮ１８１６に通信可能に結合され得る。また、ＳＳＨ　ＶＣＮ１８１２は、ＬＰＧ１８１０を介して、データプレーンＶＣＮ１８１８に通信可能に結合され得る。制御プレーンＶＣＮ１８１６およびデータプレーンＶＣＮ１８１８は、ＩａａＳプロバイダによって所有および／または操作され得るサービステナンシ１８１９に含まれ得る。

【０２４３】

制御プレーンＶＣＮ１８１６は、境界ネットワーク（例えば、企業イントラネットと外部ネットワークの間の企業ネットワークの一部）として機能する制御プレーン非武装ゾーン（ＤＭＺ：demilitarized zone）層１８２０を含むことができる。ＤＭＺに基づくサーバは、制限された責任を有し、セキュリティ侵害を封じ込められた状態に保つのに役立つことができる。さらに、ＤＭＺ層１８２０は、１つまたは複数のロードバランサ（ＬＢ：load balancer）サブネット１８２２、アプリサブネット１８２６を含むことができる制御プレーンアプリ層１８２４、データベース（ＤＢ：database）サブネット１８３０（例えば、フロントエンドＤＢサブネットおよび／またはバックエンドＤＢサブネット）を含むことができる制御プレーンデータ層１８２８を含むことができる。制御プレーンＤＭＺ層１８２０に含まれているＬＢサブネット１８２２は、制御プレーンＶＣＮ１８１６に含まれ得る制御プレーンアプリ層１８２４に含まれているアプリサブネット１８２６およびインターネットゲートウェイ１８３４に通信可能に結合されることが可能であり、アプリサブネット１８２６は、制御プレーンデータ層１８２８に含まれているＤＢサブネット１８３０ならびにサービスゲートウェイ１８３６およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１８３８に通信可能に結合され得る。制御プレーンＶＣＮ１８１６は、サービスゲートウェイ１８３６およびＮＡＴゲートウェイ１８３８を含むことができる。

【０２４４】

制御プレーンＶＣＮ１８１６は、アプリサブネット１８２６を含むことができるデータプレーンミラーアプリ層１８４０を含むことができる。データプレーンミラーアプリ層１８４０に含まれているアプリサブネット１８２６は、計算インスタンス１８４４を実行することができる仮想ネットワークインターフェイスコントローラ（ＶＮＩＣ：virtual network interface controller）１８４２を含むことができる。計算インスタンス１８４４は、データプレーンミラーアプリ層１８４０のアプリサブネット１８２６を、データプレーンアプリ層１８４６に含まれ得るアプリサブネット１８２６に通信可能に結合することができる。

【０２４５】

データプレーンＶＣＮ１８１８は、データプレーンアプリ層１８４６、データプレーンＤＭＺ層１８４８、およびデータプレーンデータ層１８５０を含むことができる。データプレーンＤＭＺ層１８４８は、データプレーンアプリ層１８４６のアプリサブネット１８２６およびデータプレーンＶＣＮ１８１８のインターネットゲートウェイ１８３４に通信可能に結合され得るＬＢサブネット１８２２を含むことができる。アプリサブネット１８２６は、データプレーンＶＣＮ１８１８のサービスゲートウェイ１８３６およびデータプレーンＶＣＮ１８１８のＮＡＴゲートウェイ１８３８に通信可能に結合され得る。データプレーンデータ層１８５０は、データプレーンアプリ層１８４６のアプリサブネット１８２６に通信可能に結合され得るＤＢサブネット１８３０を含むこともできる。

【０２４６】

制御プレーンＶＣＮ１８１６の、およびデータプレーンＶＣＮ１８１８のインターネットゲートウェイ１８３４は、パブリックインターネット１８５４に通信可能に結合され得るメタデータ管理サービス１８５２に通信可能に結合され得る。パブリックインターネッ

ト１８５４は、制御プレーンＶＣＮ１８１６の、およびデータプレーンＶＣＮ１８１８のＮＡＴゲートウェイ１８３８に通信可能に結合され得る。制御プレーンＶＣＮ１８１６の、およびデータプレーンＶＣＮ１８１８のサービスゲートウェイ１８３６は、クラウドサービス１８５６に通信可能に結合され得る。

【０２４７】

一部の例では、制御プレーンＶＣＮ１８１６の、またはデータプレーンＶＣＮ１８１８のサービスゲートウェイ１８３６は、パブリックインターネット１８５４を通らずに、クラウドサービス１８５６へのアプリケーションプログラミングインターフェイス（ＡＰＩ：application programming interface）呼び出しを行うことができる。サービスゲートウェイ１８３６からクラウドサービス１８５６へのＡＰＩ呼び出しは、一方向であることができ、サービスゲートウェイ１８３６は、クラウドサービス１８５６へのＡＰＩ呼び出しを行うことができ、クラウドサービス１８５６は、要求されたデータをサービスゲートウェイ１８３６に送信することができる。しかし、クラウドサービス１８５６は、サービスゲートウェイ１８３６へのＡＰＩ呼び出しを開始しなくてよい。

【０２４８】

一部の例では、セキュアホストテナンシ１８０４は、サービステナンシ１８１９に直接接続されることが可能であり、そうでなければ、分離されてよい。セキュアホストサブネット１８０８は、ＬＰＧ１８１０を介してＳＳＨサブネット１８１４と通信することができ、ＬＰＧ１８１０は、そうしないと分離されたシステム上で、双方向通信を可能にすることができる。セキュアホストサブネット１８０８をＳＳＨサブネット１８１４に接続することは、セキュアホストサブネット１８０８に、サービステナンシ１８１９内の他の実体へのアクセスを与えてよい。

【０２４９】

制御プレーンＶＣＮ１８１６は、サービステナンシ１８１９のユーザが、望ましいリソースを設定するか、またはそうでなければ、プロビジョニングすることを可能にしてよい。制御プレーンＶＣＮ１８１６内でプロビジョニングされた望ましいリソースは、データプレーンＶＣＮ１８１８においてデプロイされるか、またはそうでなければ、使用されてよい。一部の例では、制御プレーンＶＣＮ１８１６は、データプレーンＶＣＮ１８１８から分離されることが可能であり、制御プレーンＶＣＮ１８１６のデータプレーンミラーアプリ層１８４０は、データプレーンミラーアプリ層１８４０およびデータプレーンアプリ層１８４６に含まれ得るＶＮＩＣ１８４２を介して、データプレーンＶＣＮ１８１８のデータプレーンアプリ層１８４６と通信することができる。

【０２５０】

一部の例では、システムのユーザまたは顧客は、要求をメタデータ管理サービス１８５２に伝達することができるパブリックインターネット１８５４を介して、要求、例えば、作成、読み取り、更新、または削除（ＣＲＵＤ：create, read, update, or delete）操作を行うことができる。メタデータ管理サービス１８５２は、インターネットゲートウェイ１８３４を介して、要求を制御プレーンＶＣＮ１８１６に伝達することができる。要求は、制御プレーンＤＭＺ層１８２０に含まれているＬＢサブネット１８２２によって受信され得る。ＬＢサブネット１８２２は、要求が有効であるということを決定してよく、この決定に応答して、ＬＢサブネット１８２２は、要求を、制御プレーンアプリ層１８２４に含まれているアプリサブネット１８２６に送信することができる。要求の妥当性が確認され、要求がパブリックインターネット１８５４への呼び出しを必要とする場合、パブリックインターネット１８５４への呼び出しが、パブリックインターネット１８５４への呼び出しを行うことができるＮＡＴゲートウェイ１８３８に送信されてよい。要求によって格納されるのが望ましいことがあるメモリが、ＤＢサブネット１８３０内で格納され得る。

【０２５１】

一部の例では、データプレーンミラーアプリ層１８４０は、制御プレーンＶＣＮ１８１６とデータプレーンＶＣＮ１８１８の間の直接通信を容易にすることができる。例えば、

構成に対する変更、更新、または他の適切な修正が、データプレーンＶＣＮ１８１８に含まれているリソースに適用されるのが望ましいことがある。ＶＮＩＣ１８４２を介して、制御プレーンＶＣＮ１８１６は、データプレーンＶＣＮ１８１８に含まれているリソースと直接通信し、それによって、リソースの構成に対する変更、更新、または他の適切な修正を実行することができる。

【０２５２】

一部の実施形態では、制御プレーンＶＣＮ１８１６およびデータプレーンＶＣＮ１８１８は、サービステナンシ１８１９に含まれ得る。この場合、システムのユーザまたは顧客は、制御プレーンＶＣＮ１８１６またはデータプレーンＶＣＮ１８１８のいずれかを、所有することも、操作することも行わなくてよい。代わりに、ＩａａＳプロバイダが、両方ともサービステナンシ１８１９に含まれ得る制御プレーンＶＣＮ１８１６およびデータプレーンＶＣＮ１８１８を所有するか、または操作してよい。この実施形態は、ユーザまたは顧客が他のユーザのリソースまたは他の顧客のリソースと情報をやりとりするのを防ぐことができる、ネットワークの分離を可能にすることができる。また、この実施形態は、システムのユーザまたは顧客が、格納のために、望ましいレベルのセキュリティを有さないことがあるパブリックインターネット１８５４に頼ることを必要とせずに、データベースをプライベートに格納することを可能にしてよい。

【０２５３】

他の実施形態では、制御プレーンＶＣＮ１８１６に含まれているＬＢサブネット１８２２は、サービスゲートウェイ１８３６から信号を受信するように構成され得る。この実施形態では、制御プレーンＶＣＮ１８１６およびデータプレーンＶＣＮ１８１８は、パブリックインターネット１８５４を呼び出さずに、ＩａａＳプロバイダの顧客によって呼び出されるように構成されてよい。ＩａａＳプロバイダの顧客は、顧客が使用するデータベースが、ＩａａＳプロバイダによって制御されることがあり、パブリックインターネット１８５４から分離され得るサービステナンシ１８１９に格納されることがあるため、この実施形態を望むことがある。

【０２５４】

図１９は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別の例示的なパターンを示すブロック図１９００である。サービスオペレータ１９０２（例えば、図１８のサービスオペレータ１８０２）は、仮想クラウドネットワーク（ＶＣＮ）１９０６（例えば、図１８のＶＣＮ１８０６）およびセキュアホストサブネット１９０８（例えば、図１８のセキュアホストサブネット１８０８）を含むことができるセキュアホストテナンシ１９０４（例えば、図１８のセキュアホストテナンシ１８０４）に通信可能に結合され得る。ＶＣＮ１９０６は、セキュアシェル（ＳＳＨ）ＶＣＮ１９１２に含まれているローカルピアリングゲートウェイ（ＬＰＧ）１８１０を介してＳＳＨ　ＶＣＮ１９１２（例えば、図１８のＳＳＨ　ＶＣＮ１８１２）に通信可能に結合され得る、ＬＰＧ１９１０（例えば、図１８のＬＰＧ１８１０）を含むことができる。ＳＳＨ　ＶＣＮ１９１２はＳＳＨサブネット１９１４（例えば、図１８のＳＳＨサブネット１８１４）を含むことができ、ＳＳＨ　ＶＣＮ１９１２は、制御プレーンＶＣＮ１９１６に含まれているＬＰＧ１９１０を介して、制御プレーンＶＣＮ１９１６（例えば、図１８の制御プレーンＶＣＮ１８１６）に通信可能に結合され得る。制御プレーンＶＣＮ１９１６は、サービステナンシ１９１９（例えば、図１８のサービステナンシ１８１９）に含まれることが可能であり、データプレーンＶＣＮ１９１８（例えば、図１８のデータプレーンＶＣＮ１８１８）は、システムのユーザまたは顧客によって所有または操作され得る顧客のテナンシ１９２１に含まれることが可能である。

【０２５５】

制御プレーンＶＣＮ１９１６は、ＬＢサブネット１９２２（例えば、図１８のＬＢサブネット１８２２）を含むことができる制御プレーンＤＭＺ層１９２０（例えば、図１８の制御プレーンＤＭＺ層１８２０）、アプリサブネット１９２６（例えば、図１８のアプリサブネット１８２６）を含むことができる制御プレーンアプリ層１９２４（例えば、図１

８の制御プレーンアプリ層１８２４）、データベース（ＤＢ）サブネット１９３０（例えば、図１８のデータベース（ＤＢ）サブネット１８３０に類似する）を含むことができる制御プレーンデータ層１９２８（例えば、図１８の制御プレーンデータ層１８２８）を含むことができる。制御プレーンＤＭＺ層１９２０に含まれているＬＢサブネット１９２２は、制御プレーンＶＣＮ１９１６に含まれ得る制御プレーンアプリ層１９２４に含まれているアプリサブネット１９２６およびインターネットゲートウェイ１９３４（例えば、図１８のインターネットゲートウェイ１８３４）に通信可能に結合されることが可能であり、アプリサブネット１９２６は、制御プレーンデータ層１９２８に含まれているＤＢサブネット１９３０ならびにサービスゲートウェイ１９３６（例えば、図１８のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１９３８（例えば、図１８のＮＡＴゲートウェイ１８３８）に通信可能に結合され得る。制御プレーンＶＣＮ１９１６は、サービスゲートウェイ１９３６およびＮＡＴゲートウェイ１９３８を含むことができる。

【０２５６】

制御プレーンＶＣＮ１９１６は、アプリサブネット１９２６を含むことができるデータプレーンミラーアプリ層１９４０（例えば、図１８のデータプレーンミラーアプリ層１８４０）を含むことができる。データプレーンミラーアプリ層１９４０に含まれているアプリサブネット１９２６は、計算インスタンス１９４４（例えば、図１８の計算インスタンス１８４４に類似する）を実行することができる仮想ネットワークインターフェイスコントローラ（ＶＮＩＣ）１９４２（例えば、１８４２のＶＮＩＣ）を含むことができる。計算インスタンス１９４４は、データプレーンミラーアプリ層１９４０に含まれているＶＮＩＣ１９４２およびデータプレーンアプリ層１９４６に含まれているＶＮＩＣ１９４２を介して、データプレーンミラーアプリ層１９４０のアプリサブネット１９２６とデータプレーンアプリ層１９４６（例えば、図１８のデータプレーンアプリ層１８４６）に含まれ得るアプリサブネット１９２６の間の通信を容易にすることができる。

【０２５７】

制御プレーンＶＣＮ１９１６に含まれているインターネットゲートウェイ１９３４は、パブリックインターネット１９５４（例えば、図１８のパブリックインターネット１８５４）に通信可能に結合され得るメタデータ管理サービス１９５２（例えば、図１８のメタデータ管理サービス１８５２）に通信可能に結合され得る。パブリックインターネット１９５４は、制御プレーンＶＣＮ１９１６に含まれているＮＡＴゲートウェイ１９３８に通信可能に結合され得る。制御プレーンＶＣＮ１４１６に含まれているサービスゲートウェイ１９３６は、クラウドサービス１９５６（例えば、図１８のクラウドサービス１８５６）に通信可能に結合され得る。

【０２５８】

一部の例では、データプレーンＶＣＮ１９１８は、顧客のテナンシ１９２１に含まれ得る。この場合、ＩａａＳプロバイダは、顧客ごとに制御プレーンＶＣＮ１９１６を提供してよく、ＩａａＳプロバイダは、顧客ごとに、サービステナンシ１９１９に含まれている固有の計算インスタンス１９４４を設定してよい。各計算インスタンス１９４４は、サービステナンシ１９１９に含まれている制御プレーンＶＣＮ１９１６と顧客のテナンシ１９２１に含まれているデータプレーンＶＣＮ１９１８の間の通信を可能にしてよい。計算インスタンス１９４４は、サービステナンシ１９１９に含まれている制御プレーンＶＣＮ１９１６内でプロビジョニングされているリソースが、顧客のテナンシ１９２１に含まれているデータプレーンＶＣＮ１９１８においてデプロイされること、またはそうでなければ、使用されることを可能にしてよい。

【０２５９】

他の例では、ＩａａＳプロバイダの顧客は、顧客のテナンシ１９２１に存続するデータベースを保有してよい。この例では、制御プレーンＶＣＮ１９１６は、アプリサブネット１９２６を含むことができるデータプレーンミラーアプリ層１９４０を含むことができる。データプレーンミラーアプリ層１９４０は、データプレーンＶＣＮ１９１８に存在する

ことができるが、データプレーンミラーアプリ層１９４０は、データプレーンＶＣＮ１９１８に存続しなくてよい。すなわち、データプレーンミラーアプリ層１９４０は、顧客のテナンシ１９２１に対するアクセス権限を有してよいが、データプレーンミラーアプリ層１９４０は、データプレーンＶＣＮ１９１８に存在しなくてよく、ＩａａＳプロバイダの顧客によって所有されることも操作されることもなくてよい。データプレーンミラーアプリ層１９４０は、データプレーンＶＣＮ１９１８への呼び出しを行うように構成されてよいが、制御プレーンＶＣＮ１９１６に含まれているいずれかの実体への呼び出しを行うように構成されなくてよい。顧客は、制御プレーンＶＣＮ１９１６内でプロビジョニングされているデータプレーンＶＣＮ１９１８内のリソースをデプロイすること、またはそうでなければ、使用することを望むことがあり、データプレーンミラーアプリ層１９４０は、顧客のリソースの望ましいデプロイメントまたは他の使用を容易にすることができる。

【０２６０】

一部の実施形態では、ＩａａＳプロバイダの顧客は、フィルタをデータプレーンＶＣＮ１９１８に適用することができる。この実施形態では、顧客は、どのデータプレーンＶＣＮ１９１８がアクセスできるかを決定することができ、顧客は、データプレーンＶＣＮ１９１８からパブリックインターネット１９５４へのアクセスを制限してよい。ＩａａＳプロバイダは、フィルタを適用すること、またはそうでなければ、任意の外部のネットワークまたはデータベースへのデータプレーンＶＣＮ１９１８のアクセスを制御することが、できなくてよい。顧客によってフィルタおよび制御を顧客のテナンシ１９２１に含まれているデータプレーンＶＣＮ１９１８に適用することは、他の顧客から、およびパブリックインターネット１９５４から、データプレーンＶＣＮ１９１８を分離するのに役立つことができる。

【０２６１】

一部の実施形態では、クラウドサービス１９５６は、パブリックインターネット１９５４、制御プレーンＶＣＮ１９１６、またはデータプレーンＶＣＮ１９１８に存在しないことがあるサービスにアクセスするために、サービスゲートウェイ１９３６によって呼び出され得る。クラウドサービス１９５６と制御プレーンＶＣＮ１９１６またはデータプレーンＶＣＮ１９１８との間の接続は、作動中であることも、継続的であることもなくてよい。クラウドサービス１９５６は、ＩａａＳプロバイダによって所有または操作される異なるネットワークに存在してよい。クラウドサービス１９５６は、サービスゲートウェイ１９３６からの呼び出しを受信するように構成されてよく、パブリックインターネット１９５４からの呼び出しを受信しないように構成されてよい。一部のクラウドサービス１９５６は、他のクラウドサービス１９５６から分離されてよく、制御プレーンＶＣＮ１９１６は、制御プレーンＶＣＮ１９１６と同じリージョンに存在しないことがあるクラウドサービス１９５６から分離されてよい。例えば、制御プレーンＶＣＮ１９１６が「リージョン１」に位置することがあり、クラウドサービスの「デプロイメント１３」がリージョン１および「リージョン２」に位置することがある。リージョン１に位置する制御プレーンＶＣＮ１９１６に含まれているサービスゲートウェイ１９３６によってデプロイメント１３への呼び出しが行われる場合、この呼び出しは、リージョン１内のデプロイメント１３に送信されてよい。この例では、制御プレーンＶＣＮ１９１６、またはリージョン１内のデプロイメント１３は、リージョン２内のデプロイメント１３に通信可能に結合されること、またはそうでなければ、リージョン２内のデプロイメント１３と通信することがなくてよい。

【０２６２】

図２０は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別の例示的なパターンを示すブロック図２０００である。サービスオペレータ２００２（例えば、図１８のサービスオペレータ１８０２）は、仮想クラウドネットワーク（ＶＣＮ）２００６（例えば、図１８のＶＣＮ１８０６）およびセキュアホストサブネット２００８（例えば、図１８のセキュアホストサブネット１８０８）を含むことができるセキュアホストテナンシ２００４（例えば、図１８のセキュアホストテナンシ１８０４）に通信可能に結合され

得る。ＶＣＮ２００６は、ＳＳＨ　ＶＣＮ２０１２に含まれているＬＰＧ２０１０を介してＳＳＨ　ＶＣＮ２０１２（例えば、図１８のＳＳＨ　ＶＣＮ１８１２）に通信可能に結合され得る、ＬＰＧ２０１０（例えば、図１８のＬＰＧ１８１０）を含むことができる。ＳＳＨ　ＶＣＮ２０１２はＳＳＨサブネット２０１４（例えば、図１８のＳＳＨサブネット１８１４）を含むことができ、ＳＳＨ　ＶＣＮ１８１２は、制御プレーンＶＣＮ２０１６に含まれているＬＰＧ２０１０を介して制御プレーンＶＣＮ２０１６（例えば、図１８の制御プレーンＶＣＮ１８１６）に、およびデータプレーンＶＣＮ２０１８に含まれているＬＰＧ２０１０を介してデータプレーンＶＣＮ２０１８（例えば、図１８のデータプレーン１８１８）に、通信可能に結合され得る。制御プレーンＶＣＮ２０１６およびデータプレーンＶＣＮ２０１８は、サービステナンシ２０１９（例えば、図１８のサービステナンシ１８１９）に含まれ得る。

【０２６３】

制御プレーンＶＣＮ１８１６は、ロードバランサ（ＬＢ）サブネット１８２２（例えば、図１８のＬＢサブネット１８２２）を含むことができる制御プレーンＤＭＺ層１８２０（例えば、図１８の制御プレーンＤＭＺ層１８２０）、アプリサブネット２０２６（例えば、図１８のアプリサブネット１８２６に類似する）を含むことができる制御プレーンアプリ層２０２４（例えば、図１８の制御プレーンアプリ層１８２４）、ＤＢサブネット２０３０を含むことができる制御プレーンデータ層２０２８（例えば、図１８の制御プレーンデータ層１８２８）を含むことができる。制御プレーンＤＭＺ層２０２０に含まれているＬＢサブネット２０２２は、制御プレーンＶＣＮ２０１６に含まれ得る制御プレーンアプリ層２０２４に含まれているアプリサブネット２０２６に、およびインターネットゲートウェイ１８３４（例えば、図１８のインターネットゲートウェイ１８３４）に通信可能に結合されることが可能であり、アプリサブネット２０２６は、制御プレーンデータ層１８２８に含まれているＤＢサブネット１８３０に、ならびにサービスゲートウェイ１８３６（例えば、図１８のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ１８３８（例えば、図１８のＮＡＴゲートウェイ１８３８）に通信可能に結合され得る。制御プレーンＶＣＮ２０１６は、サービスゲートウェイ２０３６およびＮＡＴゲートウェイ２０３８を含むことができる。

【０２６４】

データプレーンＶＣＮ２０１８は、データプレーンアプリ層２０４６（例えば、図１８のデータプレーンアプリ層１８４６）、データプレーンＤＭＺ層２０４８（例えば、図１８のデータプレーンＤＭＺ層１８４８）、およびデータプレーンデータ層２０５０（例えば、図１８のデータプレーンデータ層１８５０）を含むことができる。データプレーンＤＭＺ層２０４８は、データプレーンアプリ層２０４６の信頼できるアプリサブネット２０６０および信頼できないアプリサブネット２０６２ならびにデータプレーンＶＣＮ２０１８に含まれているインターネットゲートウェイ２０３４に通信可能に結合され得るＬＢサブネット２０２２を含むことができる。信頼できるアプリサブネット２０６０は、データプレーンＶＣＮ２０１８に含まれているサービスゲートウェイ２０３６、データプレーンＶＣＮ２０１８に含まれているＮＡＴゲートウェイ２０３８、およびデータプレーンデータ層２０５０に含まれているＤＢサブネット２０３０に、通信可能に結合され得る。信頼できないアプリサブネット２０６２は、データプレーンＶＣＮ２０１８に含まれているサービスゲートウェイ２０３６、およびデータプレーンデータ層２０５０に含まれているＤＢサブネット２０３０に、通信可能に結合され得る。データプレーンデータ層２０５０は、データプレーンＶＣＮ２０１８に含まれているサービスゲートウェイ２０３６に通信可能に結合され得るＤＢサブネット２０３０を含むことができる。

【０２６５】

信頼できないアプリサブネット２０６２は、テナント仮想マシン（ＶＭ）２０６６（１）～（Ｎ）に通信可能に結合され得る１つまたは複数のプライマリＶＮＩＣ２０６４（１）～（Ｎ）を含むことができる。各テナントＶＭ２０６６（１）～（Ｎ）は、それぞれの顧客のテナンシ２０７０（１）～（Ｎ）に含まれ得るそれぞれのコンテナ出口ＶＣＮ２０

６８（１）～（Ｎ）に含まれ得るそれぞれのアプリサブネット２０６７（１）～（Ｎ）に、通信可能に結合され得る。それぞれのセカンダリＶＮＩＣ２０７２（１）～（Ｎ）は、データプレーンＶＣＮ２０１８に含まれている信頼できないアプリサブネット２０６２とコンテナ出口ＶＣＮ２０６８（１）～（Ｎ）に含まれているアプリサブネットの間の通信を容易にすることができる。各コンテナ出口ＶＣＮ２０６８（１）～（Ｎ）は、パブリックインターネット２０５４（例えば、図１８のパブリックインターネット１８５４）に通信可能に結合され得るＮＡＴゲートウェイ２０３８を含むことができる。

【０２６６】

制御プレーンＶＣＮ２０１６に含まれており、データプレーンＶＣＮ２０１８に含まれているインターネットゲートウェイ２０３４は、パブリックインターネット２０５４に通信可能に結合され得るメタデータ管理サービス２０５２（例えば、図１８のメタデータ管理システム１８５２）に通信可能に結合され得る。パブリックインターネット２０５４は、制御プレーンＶＣＮ２０１６に含まれており、データプレーンＶＣＮ２０１８に含まれているＮＡＴゲートウェイ２０３８に通信可能に結合され得る。制御プレーンＶＣＮ２０１６に含まれており、データプレーンＶＣＮ２０１８に含まれているサービスゲートウェイ２０３６は、クラウドサービス２０５６に通信可能に結合され得る。

【０２６７】

一部の実施形態では、データプレーンＶＣＮ２０１８は、顧客のテナンシ２０７０と統合され得る。この統合は、コードを実行するときにサポートを望むことがある場合など、場合によっては、ＩａａＳプロバイダの顧客にとって有用なまたは望ましいことであり得る。顧客は、破壊的であり得るコードを実行するために提供することがあり、他の顧客のリソースと通信することがあり、またはそうでなければ、望ましくない影響を引き起こすことがある。これに応答して、ＩａａＳプロバイダは、顧客によってＩａａＳプロバイダに与えられたコードを実行するべきかどうかを判定してよい。

【０２６８】

一部の例では、ＩａａＳプロバイダの顧客は、一時的なネットワークアクセス権限をＩａａＳプロバイダに付与し、データプレーンアプリ層２０４６に接続される機能を要求することがある。この機能を実行するためのコードは、ＶＭ２０６６（１）～（Ｎ）において実行されてよく、このコードは、データプレーンＶＣＮ２０１８上の他の場所で実行するように構成されなくてよい。各ＶＭ２０６６（１）～（Ｎ）は、１つの顧客のテナンシ２０７０に接続されてよい。ＶＭ２０６６（１）～（Ｎ）に含まれているそれぞれのコンテナ２０７１（１）～（Ｎ）は、コードを実行するように構成されてよい。この場合、二重の分離が存在することができ（例えば、コードを実行しているコンテナ２０７１（１）～（Ｎ）、コンテナ２０７１（１）～（Ｎ）は、信頼できないアプリサブネット２０６２に含まれている少なくともＶＭ２０６６（１）～（Ｎ）に含まれてよい）、これは、正しくないか、またはそうでなければ、望ましくないコードが、ＩａａＳプロバイダのネットワークに損傷を与えること、または異なる顧客のネットワークに損傷を与えることを防ぐのに役立つことができる。コンテナ２０７１（１）～（Ｎ）は、顧客のテナンシ２０７０に通信可能に結合されてよく、顧客のテナンシ２０７０との間でデータを送信または受信するように構成されてよい。コンテナ２０７１（１）～（Ｎ）は、データプレーンＶＣＮ２０１８内の任意の他の実体との間でデータを送信または受信するように構成されなくてよい。コードの実行の完了時に、ＩａａＳプロバイダは、コンテナ２０７１（１）～（Ｎ）を強制終了するか、またはそうでなければ、破棄してよい。

【０２６９】

一部の実施形態では、信頼できるアプリサブネット２０６０は、ＩａａＳプロバイダによって所有または操作され得るコードを実行してよい。この実施形態では、信頼できるアプリサブネット２０６０は、ＤＢサブネット２０３０に通信可能に結合されてよく、ＤＢサブネット２０３０内でＣＲＵＤ操作を実行するように構成されてよい。信頼できないアプリサブネット２０６２は、ＤＢサブネット２０３０に通信可能に結合されてよいが、この実施形態では、信頼できないアプリサブネットは、ＤＢサブネット２０３０内で読み取

り操作を実行するように構成されてよい。各顧客のＶＭ２０６６（１）～（Ｎ）に含まれ得る、顧客からのコードを実行できるコンテナ２０７１（１）～（Ｎ）は、ＤＢサブネット２０３０と通信可能に結合されなくてよい。

【０２７０】

他の実施形態では、制御プレーンＶＣＮ２０１６およびデータプレーンＶＣＮ２０１８は、直接、通信可能に結合されなくてよい。この実施形態では、制御プレーンＶＣＮ２０１６とデータプレーンＶＣＮ２０１８の間に、直接通信が存在しなくてよい。しかし、通信は、少なくとも１つの方法によって間接的に発生することができる。ＬＰＧ２０１０は、ＩａａＳプロバイダによって確立されてよく、制御プレーンＶＣＮ２０１６とデータプレーンＶＣＮ２０１８の間の通信を容易にすることができる。別の例では、制御プレーンＶＣＮ２０１６またはデータプレーンＶＣＮ２０１８は、サービスゲートウェイ２０３６を介して、クラウドサービス２０５６への呼び出しを行うことができる。例えば、制御プレーンＶＣＮ２０１６からクラウドサービス２０５６への呼び出しは、データプレーンＶＣＮ２０１８と通信することができるサービスに対する要求を含むことができる。

【０２７１】

図２１は、少なくとも１つの実施形態による、ＩａａＳアーキテクチャの別の例示的なパターンを示すブロック図２１００である。サービスオペレータ２１０２（例えば、図１８のサービスオペレータ１８０２）は、仮想クラウドネットワーク（ＶＣＮ）２１０６（例えば、図１８のＶＣＮ１８０６）およびセキュアホストサブネット２１０８（例えば、図１８のセキュアホストサブネット１８０８）を含むことができるセキュアホストテナンシ２１０４（例えば、図１８のセキュアホストテナンシ１８０４）に通信可能に結合され得る。ＶＣＮ２１０６は、ＳＳＨ　ＶＣＮ２１１２に含まれているＬＰＧ２１１０を介してＳＳＨ　ＶＣＮ２１１２（例えば、図１８のＳＳＨ　ＶＣＮ１８１２）に通信可能に結合され得る、ＬＰＧ２１１０（例えば、図１８のＬＰＧ１８１０）を含むことができる。ＳＳＨ　ＶＣＮ２１１２はＳＳＨサブネット２１１４（例えば、図１８のＳＳＨサブネット１８１４）を含むことができ、ＳＳＨ　ＶＣＮ２１１２は、制御プレーンＶＣＮ２１１６に含まれているＬＰＧ２１１０を介して制御プレーンＶＣＮ２１１６（例えば、図１８の制御プレーンＶＣＮ１８１６）に、およびデータプレーンＶＣＮ２１１８に含まれているＬＰＧ２１１０を介してデータプレーンＶＣＮ２１１８（例えば、図１８のデータプレーン１８１８）に、通信可能に結合され得る。制御プレーンＶＣＮ２１１６およびデータプレーンＶＣＮ２１１８は、サービステナンシ２１１９（例えば、図１８のサービステナンシ１８１９）に含まれ得る。

【０２７２】

制御プレーンＶＣＮ２１１６は、ＬＢサブネット２１２２（例えば、図１８のＬＢサブネット１８２２）を含むことができる制御プレーンＤＭＺ層２１２０（例えば、図１８の制御プレーンＤＭＺ層１８２０）、アプリサブネット２１２６（例えば、図１８のアプリサブネット１８２６）を含むことができる制御プレーンアプリ層２１２４（例えば、図１８の制御プレーンアプリ層１８２４）、ＤＢサブネット２１３０（例えば、図２０のＤＢサブネット２０３０）を含むことができる制御プレーンデータ層２１２８（例えば、図１８の制御プレーンデータ層１８２８）を含むことができる。制御プレーンＤＭＺ層２１２０に含まれているＬＢサブネット２１２２は、制御プレーンＶＣＮ２１１６に含まれ得る制御プレーンアプリ層２１２４に含まれているアプリサブネット２１２６に、およびインターネットゲートウェイ２１３４（例えば、図１８のインターネットゲートウェイ１８３４）に通信可能に結合されることが可能であり、アプリサブネット２１２６は、制御プレーンデータ層２１２８に含まれているＤＢサブネット２１３０に、ならびにサービスゲートウェイ２１３６（例えば、図１８のサービスゲートウェイ）およびネットワークアドレス変換（ＮＡＴ）ゲートウェイ２１３８（例えば、図１８のＮＡＴゲートウェイ１８３８）に通信可能に結合され得る。制御プレーンＶＣＮ２１１６は、サービスゲートウェイ２１３６およびＮＡＴゲートウェイ２１３８を含むことができる。

【０２７３】

データプレーンＶＣＮ２１１８は、データプレーンアプリ層２１４６（例えば、図１８のデータプレーンアプリ層１８４６）、データプレーンＤＭＺ層２１４８（例えば、図１８のデータプレーンＤＭＺ層２１４８）、およびデータプレーンデータ層２１５０（例えば、図１８のデータプレーンデータ層１８５０）を含むことができる。データプレーンＤＭＺ層２１４８は、データプレーンアプリ層２１４６の信頼できるアプリサブネット２１６０（例えば、図２０の信頼できるアプリサブネット２０６０）および信頼できないアプリサブネット２１６２（例えば、図２０の信頼できないアプリサブネット２０６２）ならびにデータプレーンＶＣＮ２１１８に含まれているインターネットゲートウェイ２１３４に通信可能に結合され得るＬＢサブネット２１２２を含むことができる。信頼できるアプリサブネット２１６０は、データプレーンＶＣＮ２１１８に含まれているサービスゲートウェイ２１３６、データプレーンＶＣＮ２１１８に含まれているＮＡＴゲートウェイ２１３８、およびデータプレーンデータ層２１５０に含まれているＤＢサブネット２１３０に、通信可能に結合され得る。信頼できないアプリサブネット２１６２は、データプレーンＶＣＮ２１１８に含まれているサービスゲートウェイ２１３６、およびデータプレーンデータ層２１５０に含まれているＤＢサブネット２１３０に、通信可能に結合され得る。データプレーンデータ層２１５０は、データプレーンＶＣＮ２１１８に含まれているサービスゲートウェイ２１３６に通信可能に結合され得るＤＢサブネット２１３０を含むことができる。

【０２７４】

信頼できないアプリサブネット２１６２は、信頼できないアプリサブネット２１６２内に存在するテナント仮想マシン（ＶＭ）２１６６（１）～（Ｎ）に通信可能に結合され得るプライマリＶＮＩＣ２１６４（１）～（Ｎ）を含むことができる。各テナントＶＭ２１６６（１）～（Ｎ）は、それぞれのコンテナ２１６７（１）～（Ｎ）内のコードを実行することができ、コンテナ出口ＶＣＮ２１６８に含まれ得るデータプレーンアプリ層２１４６に含まれ得るアプリサブネット２１２６に、通信可能に結合され得る。それぞれのセカンダリＶＮＩＣ２１７２（１）～（Ｎ）は、データプレーンＶＣＮ２１１８に含まれている信頼できないアプリサブネット２１６２とコンテナ出口ＶＣＮ２１６８に含まれているアプリサブネットの間の通信を容易にすることができる。コンテナ出口ＶＣＮは、パブリックインターネット２１５４（例えば、図１８のパブリックインターネット１８５４）に通信可能に結合され得るＮＡＴゲートウェイ２１３８を含むことができる。

【０２７５】

制御プレーンＶＣＮ２１１６に含まれており、データプレーンＶＣＮ２１１８に含まれているインターネットゲートウェイ２１３４は、パブリックインターネット２１５４に通信可能に結合され得るメタデータ管理サービス２１５２（例えば、図１８のメタデータ管理システム１８５２）に通信可能に結合され得る。パブリックインターネット２１５４は、制御プレーンＶＣＮ２１１６に含まれており、データプレーンＶＣＮ２１１８に含まれているＮＡＴゲートウェイ２１３８に通信可能に結合され得る。制御プレーンＶＣＮ２１１６に含まれており、データプレーンＶＣＮ２１１８に含まれているサービスゲートウェイ２１３６は、クラウドサービス２１５６に通信可能に結合され得る。

【０２７６】

一部の例では、図２１のブロック図２１００のアーキテクチャによって示されたパターンは、図２０のブロック図２０００のアーキテクチャによって示されたパターンの例外と見なされてよく、ＩａａＳプロバイダが顧客（例えば、切断されたリージョン）と直接通信することができない場合、ＩａａＳプロバイダの顧客にとって望ましいことがある。顧客ごとにＶＭ２１６６（１）～（Ｎ）に含まれているそれぞれのコンテナ２１６７（１）～（Ｎ）は、顧客によってリアルタイムにアクセスされ得る。コンテナ２１６７（１）～（Ｎ）は、コンテナ出口ＶＣＮ２１６８に含まれ得るデータプレーンアプリ層２１４６のアプリサブネット２１２６に含まれているそれぞれのセカンダリＶＮＩＣ２１７２（１）～（Ｎ）への呼び出しを行うように構成されてよい。セカンダリＶＮＩＣ２１７２（１）～（Ｎ）は、呼び出しをＮＡＴゲートウェイ２１３８に送信することができ、ＮＡＴゲー

トウェイ２１３８は、呼び出しをパブリックインターネット２１５４に送信してよい。この例では、顧客によってリアルタイムにアクセスされ得るコンテナ２１６７（１）～（Ｎ）が、制御プレーンＶＣＮ２１１６から分離されることが可能であり、データプレーンＶＣＮ２１１８に含まれている他の実体から分離され得る。コンテナ２１６７（１）～（Ｎ）は、他の顧客のリソースから分離されてもよい。

【０２７７】

他の例では、顧客は、コンテナ２１６７（１）～（Ｎ）を使用して、クラウドサービス２１５６を呼び出すことができる。この例では、顧客は、クラウドサービス２１５６に対してサービスを要求するコンテナ２１６７（１）～（Ｎ）内のコードを実行してよい。コンテナ２１６７（１）～（Ｎ）は、この要求をセカンダリＶＮＩＣ２１７２（１）～（Ｎ）に送信することができ、セカンダリＶＮＩＣ２１７２（１）～（Ｎ）は、この要求をＮＡＴゲートウェイに送信することができ、ＮＡＴゲートウェイは、この要求をパブリックインターネット２１５４に送信することができる。パブリックインターネット２１５４は、この要求を、インターネットゲートウェイ２１３４を介して、制御プレーンＶＣＮ２１１６に含まれているＬＢサブネット２１２２に送信することができる。この要求が有効であるということを決定することに応答して、ＬＢサブネットは、この要求をアプリサブネット２１２６に送信することができ、アプリサブネット２１２６は、サービスゲートウェイ２１３６を介して、この要求をクラウドサービス２１５６に送信することができる。

【０２７８】

図に示されているＩａａＳアーキテクチャ１８００、１９００、２０００、２１００が、示されているコンポーネント以外のコンポーネントを含んでよいということが、理解されるべきである。さらに、図に示されている実施形態は、本開示の実施形態を組み込むことができるクラウドインフラストラクチャシステムの単に一部の例である。一部の他の実施形態では、ＩａａＳシステムは、図に示されているコンポーネントより多いか、または少ないコンポーネントを含んでよく、２つ以上のコンポーネントを結合してよく、あるいはコンポーネントの異なる構成または配置を有してよい。

【０２７９】

ある実施形態では、本明細書に記載されたＩａａＳシステムは、セルフサービスの、サブスクリプションに基づく、弾力的に拡張可能な、信頼できる、高度に利用可能な、および安全な方法で顧客に配信される、一連のアプリケーション、ミドルウェア、およびデータベースサービスの提供を含んでよい。そのようなＩａａＳシステムの例は、本譲受人によって提供されるOracleクラウドインフラストラクチャ（ＯＣＩ）である。

【０２８０】

図２２は、本開示のさまざまな実施形態が実装され得る例示的なコンピュータシステム２２００を示している。システム２２００は、前述のコンピュータシステムのいずれかを実装するために使用されてよい。図に示されているように、コンピュータシステム２２００は、バスサブシステム２２０２を介して複数の周辺サブシステムと通信する処理ユニット２２０４を含んでいる。これらの周辺サブシステムは、処理加速ユニット２２０６、Ｉ／Ｏサブシステム２２０８、ストレージサブシステム２２１８、および通信サブシステム２２２４を含んでよい。ストレージサブシステム２２１８は、有形のコンピュータ可読ストレージ媒体２２２２およびシステムメモリ２２１０を含む。

【０２８１】

バスサブシステム２２０２は、コンピュータシステム２２００のさまざまなコンポーネントおよびサブシステムに、意図されたとおりに互いに通信させるためのメカニズムを提供する。バスサブシステム２２０２は、単一のバスとして概略的に示されているが、バスサブシステムの代替の実施形態は、複数のバスを利用してよい。バスサブシステム２２０２は、メモリバスまたはメモリコントローラ、ペリフェラルバス、およびさまざまなバスアーキテクチャのいずれかを使用するローカルバスを含む、複数の種類のバス構造のいずれかであってよい。例えば、そのようなアーキテクチャは、ＩＳＡ（Industry Standard Architecture）バス、ＭＣＡ（Micro Channel Architecture）バス、ＥＩＳＡ

（Enhanced ISA）バス、ＶＥＳＡ（Video Electronics Standards Association）ローカルバス、およびＩＥＥＥ　Ｐ１３８６．１規格で製造されたメザニンバスとして実装され得るＰＣＩ（Peripheral Component Interconnect）バスを含んでよい。

【０２８２】

１つまたは複数の集積回路（例えば、従来のマイクロプロセッサまたはマイクロコントローラ）として実装され得る処理ユニット２２０４は、コンピュータシステム２２００の動作を制御する。１つまたは複数のプロセッサが、処理ユニット２２０４に含まれてよい。これらのプロセッサは、シングルコアプロセッサまたはマルチコアプロセッサを含んでよい。ある実施形態では、処理ユニット２２０４は、１つまたは複数の独立した処理ユニット２２３２および／または２２３４として実装されてよく、シングルコアプロセッサまたはマルチコアプロセッサが各処理ユニットに含まれている。他の実施形態では、処理ユニット２２０４は、２つのデュアルコアプロセッサを単一のチップに統合することによって形成されたクアッドコア処理ユニットとして実装されてもよい。

【０２８３】

さまざまな実施形態では、処理ユニット２２０４は、プログラムコードに応じてさまざまなプログラムを実行することができ、複数の同時に実行するプログラムまたはプロセスを維持することができる。任意の特定の時間に、実行されるプログラムコードの一部またはすべてが、プロセッサ２２０４に、および／またはストレージサブシステム２２１８に存在することができる。適切なプログラミングによって、プロセッサ２２０４は、前述のさまざまな機能を提供することができる。コンピュータシステム２２００は、デジタル信号プロセッサ（ＤＳＰ：digital signal processor）、専用プロセッサ、および／または同様のものを含むことができる処理加速ユニット２２０６を、さらに含んでよい。

【０２８４】

Ｉ／Ｏサブシステム２２０８は、ユーザインターフェイス入力デバイスおよびユーザインターフェイス出力デバイスを含んでよい。ユーザインターフェイス入力デバイスは、キーボード、マウスまたはトラックボールなどのポインティングデバイス、ディスプレイに組み込まれたタッチパッドまたはタッチスクリーン、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、音声コマンド認識システムを備える音声入力デバイス、マイクロホン、および他の種類の入力デバイスを含んでよい。ユーザインターフェイス入力デバイスは、例えば、ユーザが、ジェスチャーおよび話されたコマンドを使用する自然なユーザインターフェイスを介して、Microsoft Xbox（登録商標）３６０ゲームコントローラなどの入力デバイスを制御して情報をやりとりすることを可能にする、Microsoft Kinect（登録商標）モーションセンサなどの、動作検出デバイスおよび／またはジェスチャー認識デバイスを含んでよい。ユーザインターフェイス入力デバイスは、ユーザの目の活動（例えば、写真を撮っているとき、および／またはメニューを選択しているときの「まばたき」）を検出し、アイジェスチャーを入力デバイス（例えば、Google Glass（登録商標））への入力として変換するGoogle Glass（登録商標）まばたき検出器などの、アイジェスチャー認識デバイスを含んでもよい。さらに、ユーザインターフェイス入力デバイスは、ユーザが音声コマンドを介して音声認識システム（例えば、Siri（登録商標）ナビゲーター）とやりとりできるようにする音声認識検出デバイスを含んでよい。

【０２８５】

ユーザインターフェイス入力デバイスは、３次元（３Ｄ：three dimensional）マウス、ジョイスティックまたはポインティングスティック、ゲームパッド、およびグラフィックタブレット、ならびにスピーカ、デジタルカメラ、デジタルビデオカメラ、ポータブルメディアプレーヤー、ウェブカメラ、画像スキャナ、指紋スキャナ、バーコードリーダ３Ｄスキャナ、３Ｄプリンタ、レーザ距離計、および視線追跡デバイスなどの、音声／視覚デバイスを含んでもよいが、これらに限定されない。さらに、ユーザインターフェイス入力デバイスは、例えば、コンピュータ断層撮影、磁気共鳴撮像、位置放出断層撮影、医用超音波検査デバイスなどの、医用画像入力デバイスを含んでよい。ユーザインターフェ

イス入力デバイスは、例えば、ＭＩＤＩキーボード、デジタル楽器などの音声入力デバイスを含んでもよい。

【０２８６】

ユーザインターフェイス出力デバイスは、ディスプレイサブシステム、インジケータライト、または音声出力デバイスなどの視覚表示以外などを含んでよい。ディスプレイサブシステムは、ブラウン管（ＣＲＴ：cathode ray tube）、液晶ディスプレイ（ＬＣＤ：liquid crystal display）またはプラズマディスプレイを使用するフラットパネルデバイスなどのフラットパネルデバイス、投射デバイス、タッチスクリーンなどであってよい。一般に、「出力デバイス」という用語の使用は、情報をコンピュータシステム２２００からユーザまたは他のコンピュータに出力するためのすべての可能性のある種類のデバイスおよびメカニズムを含むよう意図されている。例えば、ユーザインターフェイス出力デバイスは、モニタ、プリンタ、スピーカ、ヘッドホン、カーナビ、プロッター、音声出力デバイス、およびモデムなどの、テキスト情報、グラフィックス情報、および音声／ビデオ情報を視覚的に伝達するさまざまなディスプレイデバイスを含んでよいが、これらに限定されない。

【０２８７】

コンピュータシステム２２００は、システムメモリ２２１０内に現在あるように示されているソフトウェア要素を含む、ストレージサブシステム２２１８を備えてよい。システムメモリ２２１０は、処理ユニット２２０４で読み込み可能かつ実行可能なプログラム命令に加えて、これらのプログラムの実行中に生成されたデータを格納してよい。

【０２８８】

コンピュータシステム２２００の構成および種類に応じて、システムメモリ２２１０は、揮発性（ランダムアクセスメモリ（ＲＡＭ：random-access memory）など）および／または不揮発性（読み取り専用メモリ（ＲＯＭ：read-only memory）、フラッシュメモリなど）であってよい。ＲＡＭは、通常、処理ユニット２２０４によって直ちにアクセス可能である、かつ／または現在操作されて実行されているデータおよび／またはプログラムモジュールを含む。一部の実装では、システムメモリ２２１０は、スタティックランダムアクセスメモリ（ＳＲＡＭ：static random-access memory）またはダイナミックランダムアクセスメモリ（ＤＲＡＭ：dynamic random-access memory）などの、複数の異なる種類のメモリを含んでよい。一部の実装では、起動中などにコンピュータシステム２２００内の要素間で情報を転送するのに役立つ基本ルーチンを含んでいる基本入出力システム（ＢＩＯＳ：basic input/output system）が、通常はＲＯＭに格納されてよい。限定ではなく例として、システムメモリ２２１０は、クライアントアプリケーション、ウェブブラウザ、ミッドティアアプリケーション、リレーショナルデータベース管理システム（ＲＤＢＭＳ：relational database management systems）などを含んでよいアプリケーションプログラム２２１２、プログラムデータ２２１４、およびオペレーティングシステム２２１６も示している。オペレーティングシステム２２１６の例としては、Microsoft Windows（登録商標）、Apple Macintosh（登録商標）、および／またはLinuxオペレーティングシステム、さまざまな市販されているUNIX（登録商標）またはUNIXのようなオペレーティングシステム（さまざまなGNU/Linuxオペレーティングシステム、Google Chrome（登録商標）OSなどを含むが、これらに限定されない）、ならびに／あるいはiOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）17 OS、およびPalm（登録商標）OSオペレーティングシステムなどのモバイルオペレーティングシステムの、さまざまなバージョンが挙げられ得る。

【０２８９】

ストレージサブシステム２２１８は、一部の実施形態の機能を提供する基本的なプログラミングおよびデータの構成を格納するための有形のコンピュータ可読ストレージ媒体を提供してもよい。プロセッサによって実行されたときに前述の機能を提供するソフトウェア（プログラム、コードモジュール、命令）が、ストレージサブシステム２２１８に格納

されてよい。これらのソフトウェアモジュールまたは命令は、処理ユニット２２０４によって実行されてよい。ストレージサブシステム２２１８は、本開示に従って使用されるデータを格納するためのリポジトリを提供してもよい。

【０２９０】

ストレージサブシステム２２００は、コンピュータ可読ストレージ媒体２２２２にさらに接続され得るコンピュータ可読ストレージ媒体リーダ２２２０を含んでもよい。システムメモリ２２１０と組み合わせて、一緒に、任意選択的に、コンピュータ可読ストレージ媒体２２２２は、リモートの、ローカルな、固定された、および／または取り外し可能なストレージ媒体に加えて、コンピュータ可読情報を一時的に、かつ／またはより永続的に含むため、格納するため、送信するため、および取り出すためのストレージ媒体を、包括的に表してよい。

【０２９１】

コードまたはコードの一部を含んでいるコンピュータ可読ストレージ媒体２２２２は、情報の格納および／または送信のために任意の方法または技術で実装された、揮発性および不揮発性の、取り外し可能および取り外し不可能な媒体などの、ただしこれらに限定されない、ストレージ媒体および通信媒体を含む、当技術分野において知られているか、または使用されている任意の適切な媒体を含むこともできる。コンピュータ可読ストレージ媒体２２２２は、ＲＡＭ、ＲＯＭ、電子的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ：electronically erasable programmable ROM）、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ：digital versatile disk）、または他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ、または他の磁気ストレージデバイス、あるいは他の有形のコンピュータ可読媒体などの、有形のコンピュータ可読ストレージ媒体を含むことができる。コンピュータ可読ストレージ媒体２２２２は、所望の情報を送信するために使用されることが可能であり、コンピューティングシステム２２００によってアクセスされ得る、データ信号、データ送信、または任意の他の媒体などの非有形のコンピュータ可読媒体を含むこともできる。

【０２９２】

例として、コンピュータ可読ストレージ媒体２２２２は、取り外し不可能な不揮発性の磁気媒体から読み取るか、または磁気媒体に書き込むハードディスクドライブ、取り外し可能な不揮発性の磁気ディスクから読み取るか、または磁気ディスクに書き込む磁気ディスクドライブ、ならびにＣＤ　ＲＯＭ、ＤＶＤ、およびブルーレイ（登録商標）ディスク、または他の光媒体などの取り外し可能な不揮発性の光ディスクから読み取るか、または光ディスクに書き込む光ディスクドライブを含んでよい。コンピュータ可読ストレージ媒体２２２２は、Zip（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（ＵＳＢ：universal serial bus）フラッシュドライブ、セキュアデジタル（ＳＤ：secure digital）カード、ＤＶＤディスク、デジタルビデオテープなどを含んでよいが、これらに限定されない。コンピュータ可読ストレージ媒体２２２２は、フラッシュメモリベースのＳＳＤ、エンタープライズフラッシュドライブ、半導体ＲＯＭなどの、不揮発性メモリに基づく半導体ドライブ（ＳＳＤ：solid-state drives）、半導体ＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ：magneto resistive RAM）ＳＳＤなどの、揮発性メモリに基づくＳＳＤ、およびＤＲＡＭとフラッシュメモリベースのＳＳＤの組合せを使用するハイブリッドＳＳＤを含んでもよい。ディスクドライブおよび関連するコンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、およびコンピュータシステム２２００の他のデータの不揮発性ストレージを提供してよい。

【０２９３】

通信サブシステム２２２４は、他のコンピュータシステムおよびネットワークへのインターフェイスを提供する。通信サブシステム２２２４は、コンピュータシステム２２００の他のシステムからデータを受信するため、および他のシステムにデータを送信するためのインターフェイスとして機能する。例えば、通信サブシステム２２２４は、コンピュー

タシステム２２００がインターネットを介して１つまたは複数のデバイスに接続できるようにしてよい。一部の実施形態では、通信サブシステム２２２４は、ワイヤレス音声および／またはデータネットワークにアクセスするための無線周波（ＲＦ：radio frequency）トランシーバのコンポーネント（例えば、携帯電話技術、３Ｇ、４Ｇ、もしくはＥＤＧＥ（enhanced data rates for global evolution：エンハンストデータレーツフォーグローバルエボリューション）などの高度なデータネットワーク技術、Ｗｉ－Ｆｉ（ＩＥＥＥ　８０２．１１群規格、または他の移動体通信技術、あるいはこれらの任意の組合せを使用する）、全地球測位システム（ＧＰＳ：global positioning system）レシーバのコンポーネント、および／または他のコンポーネントを含むことができる。一部の実施形態では、通信サブシステム２２２４は、ワイヤレスインターフェイスに加えて、またはワイヤレスインターフェイスの代わりに、有線ネットワーク接続（例えば、イーサネット）を提供することができる。

【０２９４】

一部の実施形態では、通信サブシステム２２２４は、コンピュータシステム２２００を使用することがある１人または複数のユーザの代わりに、構造化および／または非構造化データフィード２２２６、イベントストリーム２２２８、イベント更新２２３０などの形態で入力通信を受信してもよい。

【０２９５】

例として、通信サブシステム２２２４は、Twitter（登録商標）フィード、Facebook（登録商標）の更新などのソーシャルネットワークおよび／または他の通信サービスのユーザ、リッチサイトサマリー（ＲＳＳ：Rich Site Summary）フィードなどのウェブフィード、ならびに／あるいは１つまたは複数のサードパーティの情報源からのリアルタイムの更新から、データフィード２２２６をリアルタイムに受信するように構成されてよい。

【０２９６】

さらに、通信サブシステム２２２４は、連続データストリームの形態でデータを受信するように構成されてもよく、連続データストリームは、明示的な末尾がなく、本質的に連続的であるか、または境界がなくてよいリアルタイムイベントのイベントストリーム２２２８および／またはイベント更新２２３０を含むことができる。連続データを生成するアプリケーションの例としては、例えば、センサデータアプリケーション、金融ティッカー、ネットワーク性能測定ツール（例えば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などが挙げられ得る。

【０２９７】

通信サブシステム２２２４は、構造化および／または非構造化データフィード２２２６、イベントストリーム２２２８、イベント更新２２３０などを、コンピュータシステム２２００に結合された１つまたは複数のストリーミングデータソースコンピュータと通信することができる１つまたは複数のデータベースに出力するように構成されてもよい。

【０２９８】

コンピュータシステム２２００は、ハンドヘルドポータブルデバイス（例えば、iPhone（登録商標）携帯電話、iPad（登録商標）コンピューティングタブレット、ＰＤＡ）、ウェアラブルデバイス（例えば、Google Glass（登録商標）ヘッドマウントディスプレイ）、ＰＣ、ワークステーション、メインフレーム、自動発券機、サーバラック、または任意の他のデータ処理システムを含む、さまざまな種類のうちの１つであることができる。

【０２９９】

コンピュータおよびネットワークの絶えず変化する性質のため、図に示されたコンピュータシステム２２００の説明は、単に具体的な例となるよう意図されている。図に示されたシステムよりも多いか、または少ないコンポーネントを含んでいる多くの他の構成が可能である。例えば、カスタマイズされたハードウェアが使用されてもよく、かつ／または特定の要素がハードウェア、ファームウェア、ソフトウェア（アプレットを含む）、また

はこれらの組合せにおいて実装されてよい。さらに、ネットワーク入出力デバイスなどの他のコンピューティングデバイスへの接続が採用されてよい。本明細書において提供された開示および教示に基づいて、当業者は、さまざまな実施形態を実施するための他の方法および／または方式を理解するであろう。

【０３００】

本開示の特定の実施形態が説明されたが、さまざまな修正、変更、代替の構造、および同等のものも、本開示の範囲内に包含される。本開示の実施形態は、ある特定のデータ処理環境内の動作に制限されず、複数のデータ処理環境内で自由に動作できる。さらに、特定の一連のトランザクションおよびステップを使用して本開示の実施形態が説明されたが、本開示の範囲が説明された一連のトランザクションおよびステップに限定されないということが、当業者にとって明らかであるはずである。前述の実施形態のさまざまな特徴および態様は、個別に、または一緒に使用されてよい。

【０３０１】

さらに、ハードウェアとソフトウェアの特定の組合せを使用して本開示の実施形態が説明されたが、ハードウェアとソフトウェアの他の組合せも本開示の範囲内にあるということが認識されるべきである。ハードウェアのみにおいて、またはソフトウェアのみにおいて、あるいはこれらの組合せを使用して、本開示の実施形態が実装されてよい。本明細書に記載されたさまざまなプロセスは、同じプロセッサまたは任意の組合せでの異なるプロセッサ上で実施され得る。したがって、コンポーネントまたはモジュールが、ある動作を実行するように構成されていると説明される場合、そのような構成は、例えば、この動作を実行するように電子回路を設計することによって、この動作を実行するようにプログラム可能な電子回路（マイクロプロセッサなど）をプログラムすることによって、あるいはこれらの任意の組合せによって、実現され得る。プロセスは、プロセス間通信のための従来技術を含むが、これらに限定されないさまざまな技術を使用して通信することができ、プロセスの異なる対は、異なる技術を使用してよく、またはプロセスの同じ対は、異なる時間に異なる技術を使用してよい。

【０３０２】

したがって、本明細書および図面は、限定を意味するのではなく、例示であると見なされるべきである。しかし、特許請求の範囲に示されるようなより広い思想および範囲から逸脱することなく、本明細書および図面に対して追加、削減、削除、ならびに他の修正および変更が行われてよいということが、明らかである。したがって、特定の開示の実施形態が説明されたが、これらは限定することを意図されていない。さまざまな変更および同等のものが、添付の特許請求の範囲内にある。

【０３０３】

開示された実施形態を説明する文脈における（特に、添付の特許請求の範囲の文脈における）「ａ」および「ａｎ」および「ｔｈｅ」という用語ならびに同様の指示対象の使用は、本明細書において特に示されない限り、または文脈と明らかに矛盾しない限り、単数と複数の両方を対象にすると解釈されるべきである。「備えている」、「有している」、「含んでいる（ｉｎｃｌｕｄｉｎｇ）」、および「含んでいる（ｃｏｎｔａｉｎｉｎｇ）」という用語は、特に注記されない限り、無制限の（すなわち、「～を含むが、これに限定されない」ということを意味する）用語であると解釈されるべきである。「接続される」という用語は、介在する何かが存在する場合でも、内部に部分的に、または完全に含まれるか、接続されるか、あるいは一緒に接合されると解釈されるべきである。本明細書における値の範囲の列挙は、本明細書において特に示されない限り、単に、範囲に含まれる別々の各値を個別に参照する簡単な方法として役立つよう意図されており、別々の各値は、本明細書において個別に列挙されたかのように、本明細書に組み込まれる。本明細書に記載されたすべての方法は、本明細書において特に示されない限り、または文脈と特に明確に矛盾しない限り、任意の適切な順序で実行され得る。本明細書において提供される、ありとあらゆる例、または例示的な言語（例えば、「など」）の使用は、単に、本開示の実施形態をより良く明らかにするよう意図されており、特に主張されない限り、本開示の範囲に限定を課さ

ない。本明細書における言語は、いずれかの主張されない要素を、本開示の実践にとって不可欠であるとして示すと解釈されるべきでない。

【０３０４】

「Ｘ、Ｙ、またはＺのうちの少なくとも１つ」という語句などの選言的言語は、特に明確に述べられない限り、一般に、項目、条件などが、Ｘ、Ｙ、またはＺのいずれか、あるいはこれらの任意の組合せ（例えば、Ｘ、Ｙ、および／またはＺ）であってよいということを提示するために使用されると文脈内で理解されるよう意図されている。したがって、そのような選言的言語は、一般に、ある実施形態が、Ｘのうちの少なくとも１つ、Ｙのうちの少なくとも１つ、またはＺのうちの少なくとも１つが各々存在することを必要とするということを意味するよう意図されておらず、そのようなことを意味するべきでない。

【０３０５】

本明細書では、本開示を実行するための本発明者に知られている最良のモードを含む、本開示の好ましい実施形態が説明される。前述の説明を読むときに、当業者にとって、そのような好ましい実施形態の変形が明らかになり得る。本発明者は、当業者が、必要に応じてそのような変形を採用することを期待し、本発明者は、本開示が、本明細書において詳細に説明されたような実践以外に実践されることを意図する。したがって、本開示は、適用可能な法律によって認可される、本明細書に添付されている特許請求の範囲において列挙された本主題のすべての変更および同等のものを含む。さらに、実施形態のすべての可能な変形における前述の要素の任意の組合せは、本明細書において特に示されない限り、または文脈と特に明確に矛盾しない限り、本開示によって包含される。

【０３０６】

本明細書において引用された公表文献、特許出願、および特許を含むすべての参考文献は、各参考文献が、参照によって組み込まれるように個別に詳細に示され、本明細書において全体として示された場合と同じ程度に、参照によって本明細書に組み込まれる。

【０３０７】

前述の明細書では、本明細書の特定の実施形態を参照して本開示の態様が説明されたが、当業者は、本開示がそれらに限定されないということを認識するであろう。前述の開示のさまざまな特徴および態様は、個別に、または一緒に使用されてよい。さらに、実施形態は、本明細書のより広い思想および範囲から逸脱することなく、本明細書に記載された環境および応用を越えて、任意の数の環境および応用において利用され得る。したがって、本明細書および図面は、限定ではなく例示であると見なされるべきである。

【図面】

【図１】

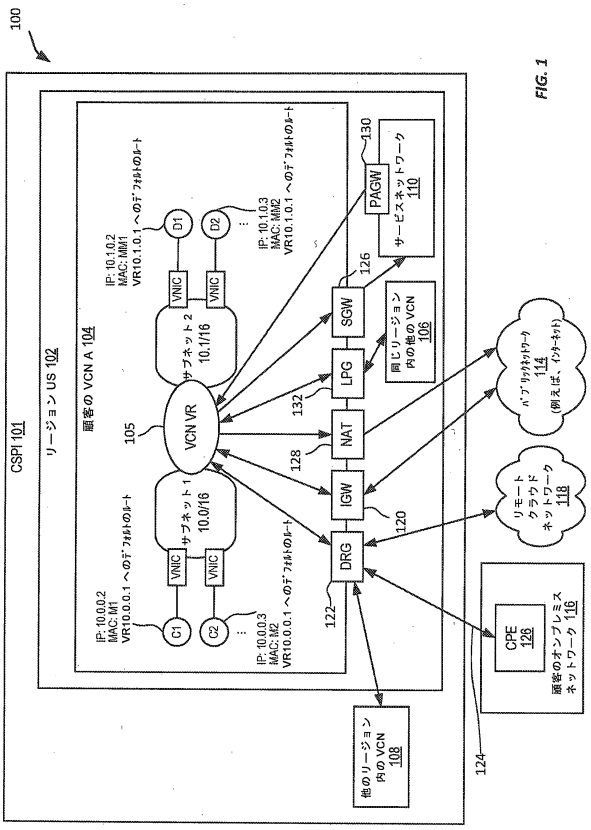

FIG. 1

【図２】

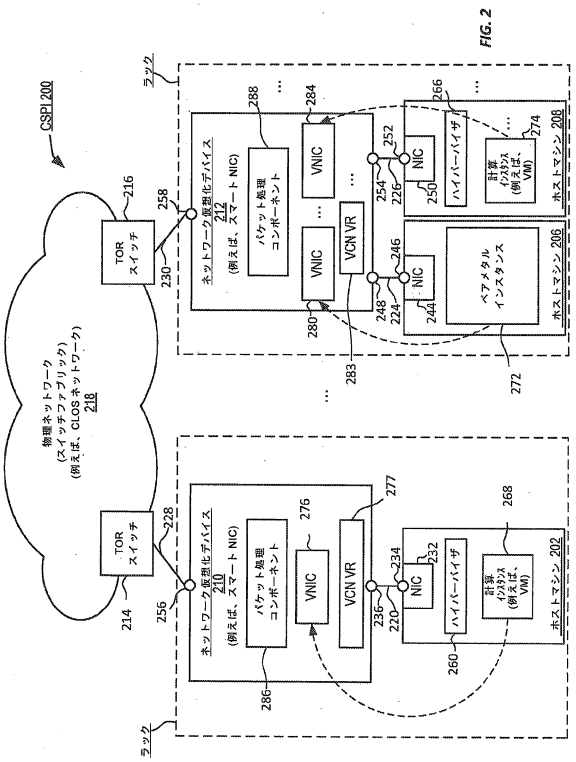

FIG. 2

【図３】

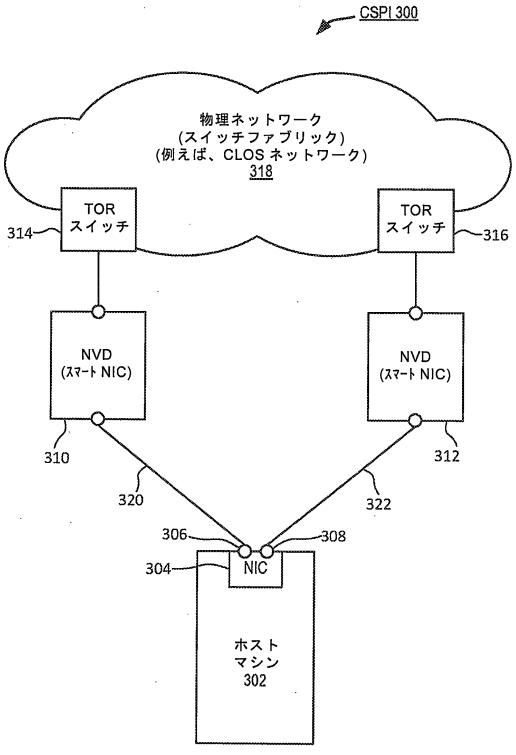

FIG. 3

【図４】

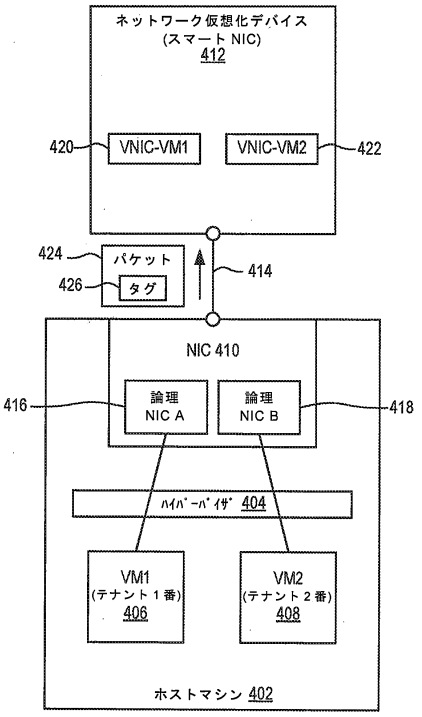

FIG. 4

【図５】

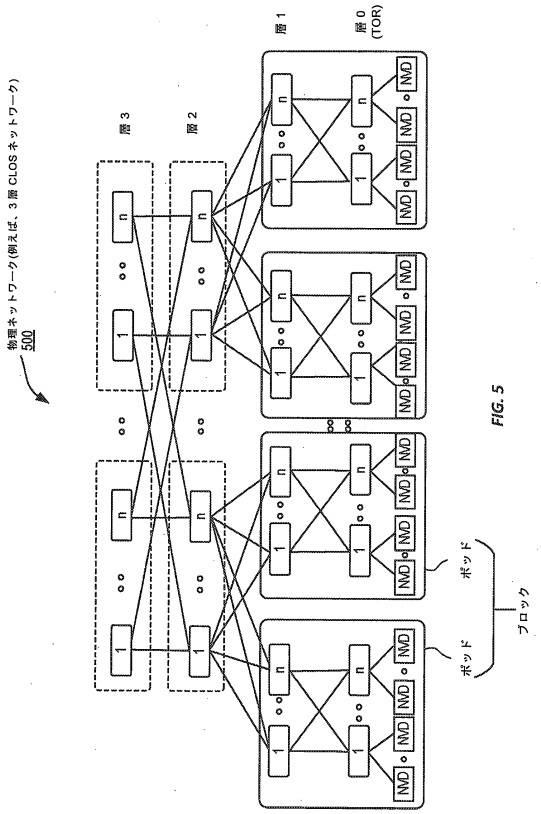

FIG. 5

【図６】

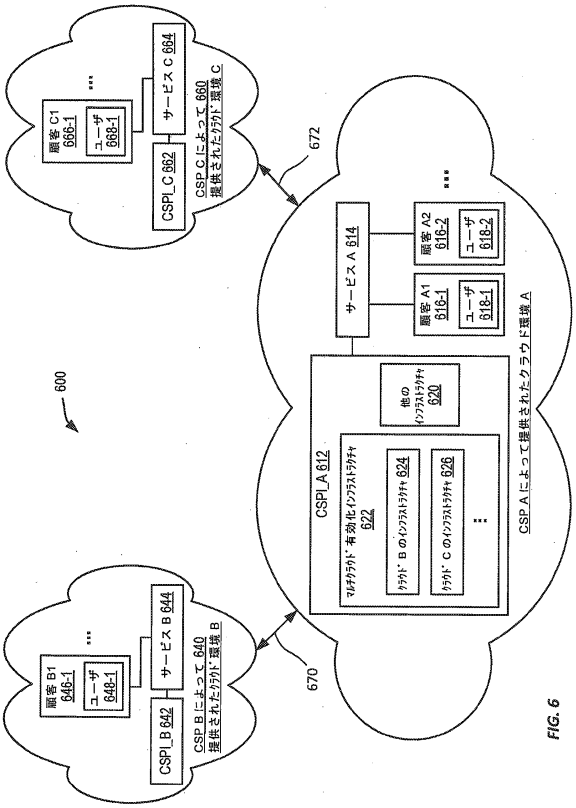

FIG. 6

【図７】

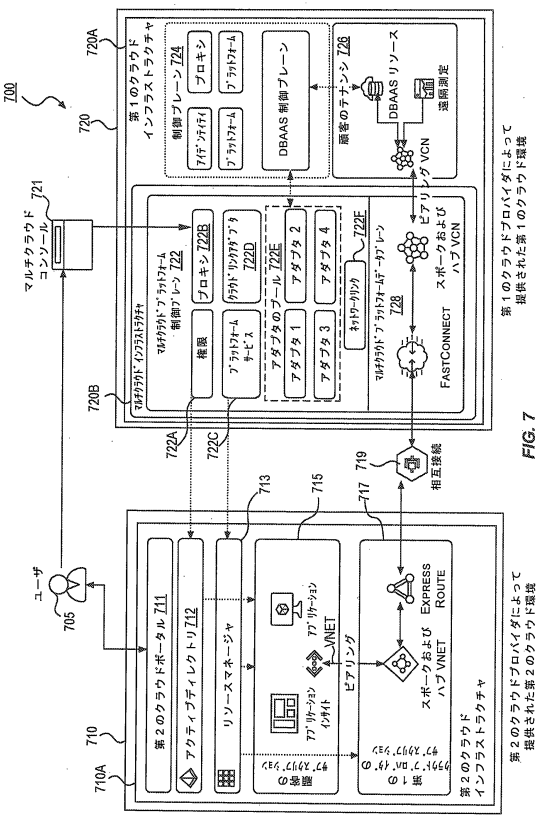

FIG. 7

【図８Ａ】

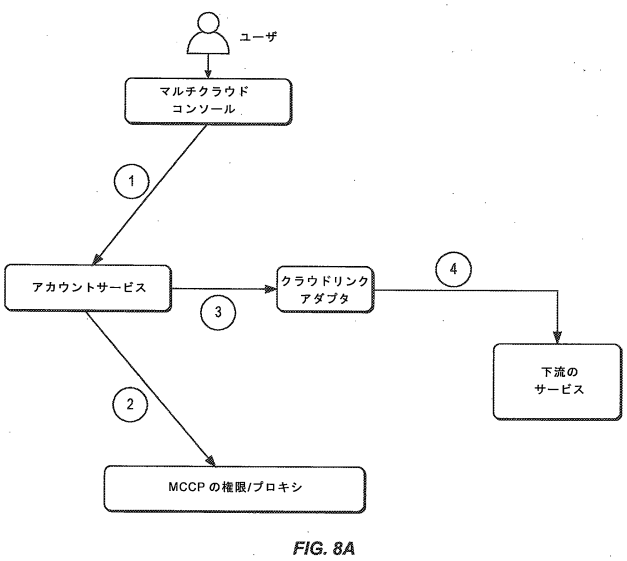

FIG. 8A

【図８Ｂ】

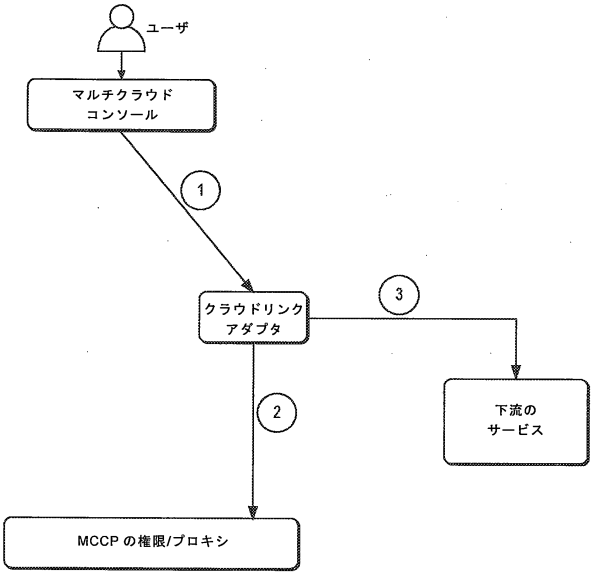

FIG. 8B

【図９】

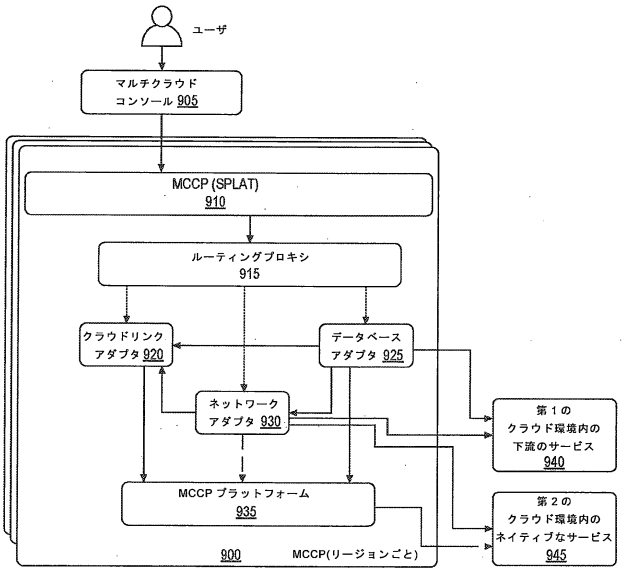

FIG. 9

【図１０】

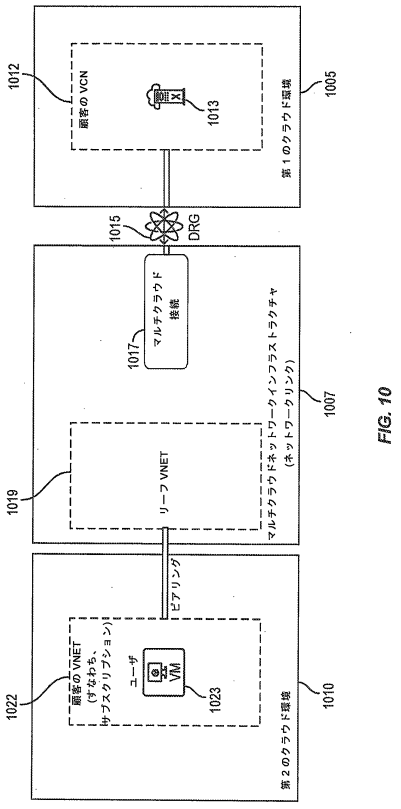

FIG. 10

【図１１－１】

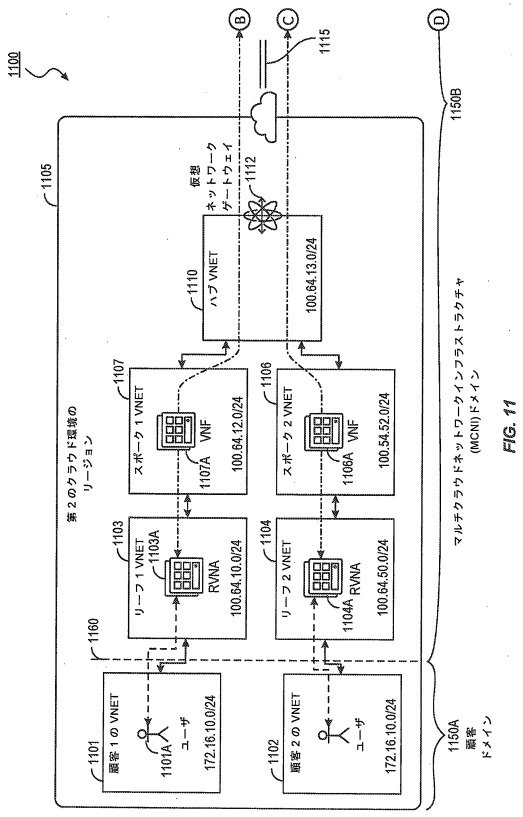

FIG. 11

【図１１－２】

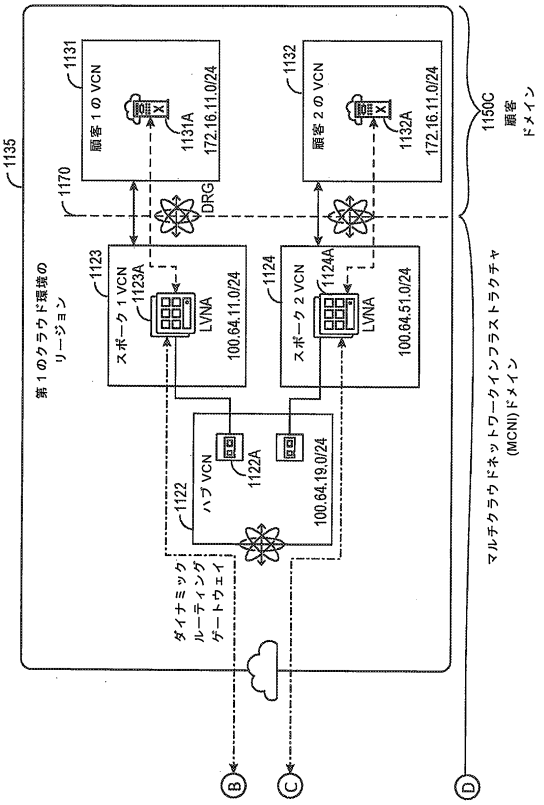

FIG. 11 (CONT.)

【図１２Ａ】

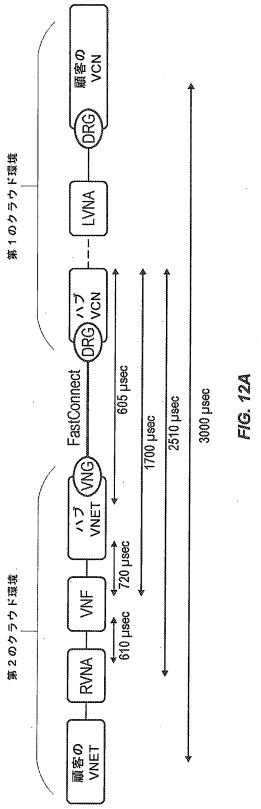

FIG. 12A

【図１２Ｂ】

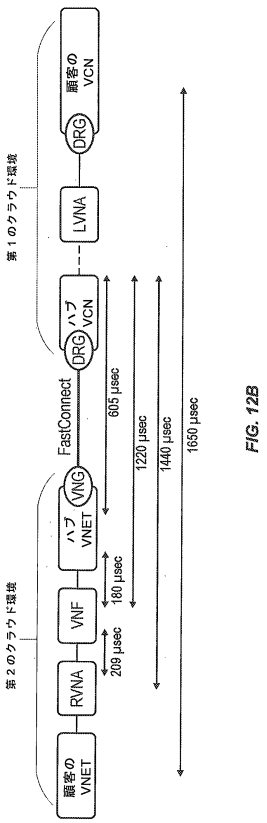

FIG. 12B

【図１２Ｃ】

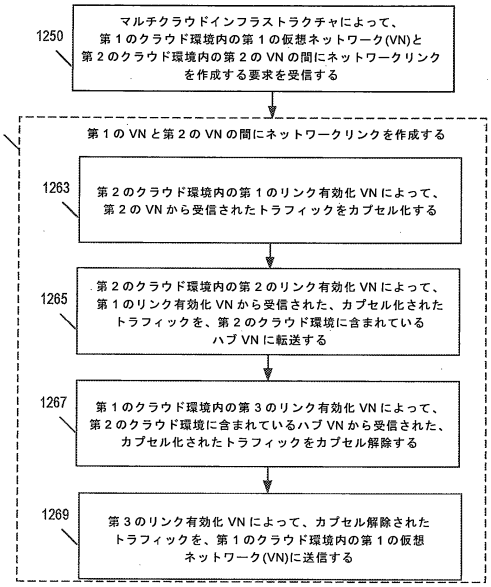

FIG. 12C

【図１３－１】

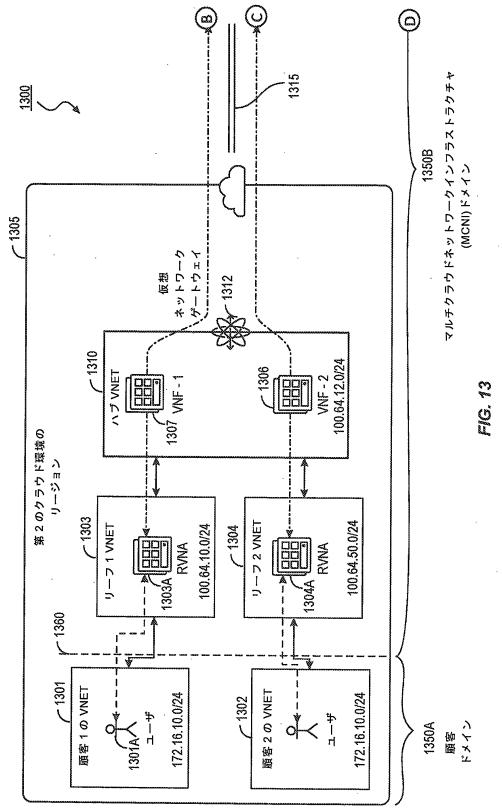

FIG. 13

【図１３－２】

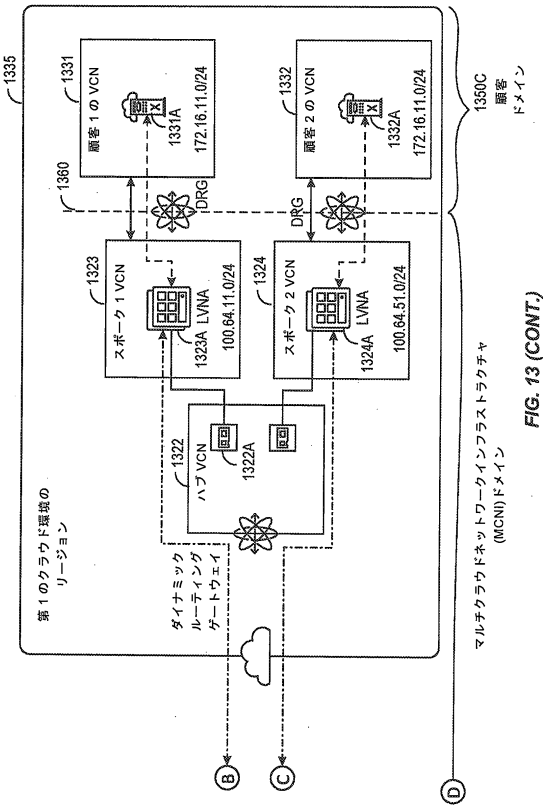

FIG. 13 (CONT.)

【図１４Ａ】

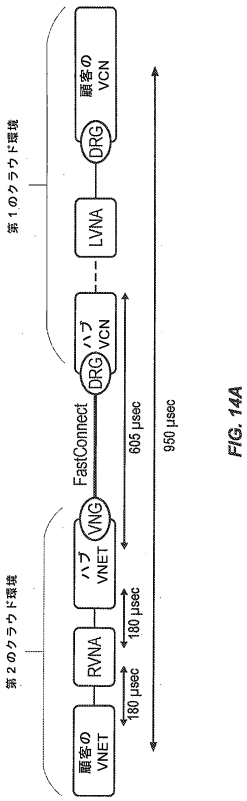

FIG. 14A

【図１４Ｂ】

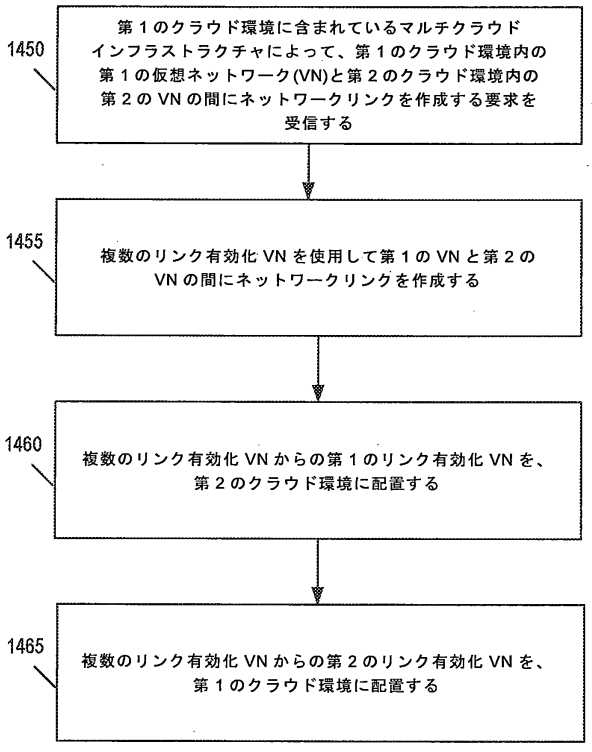

FIG. 14B

【図１５－１】

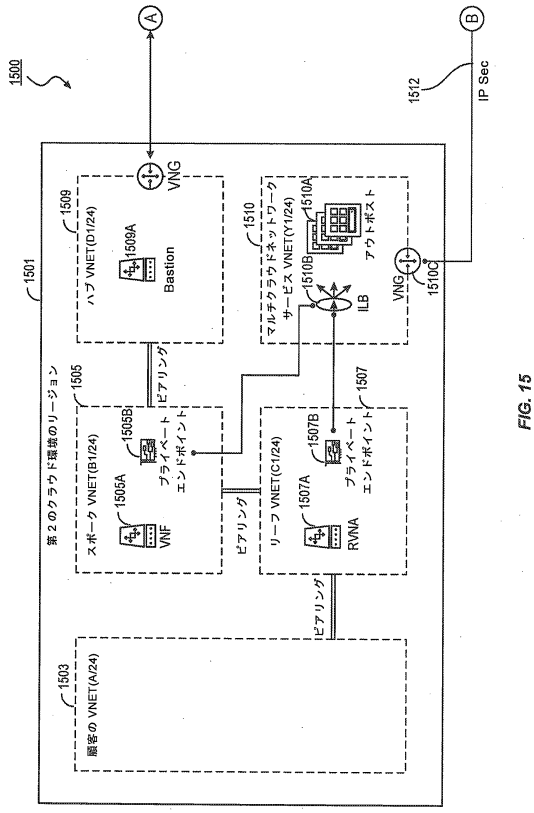

FIG. 15

【図１５－２】

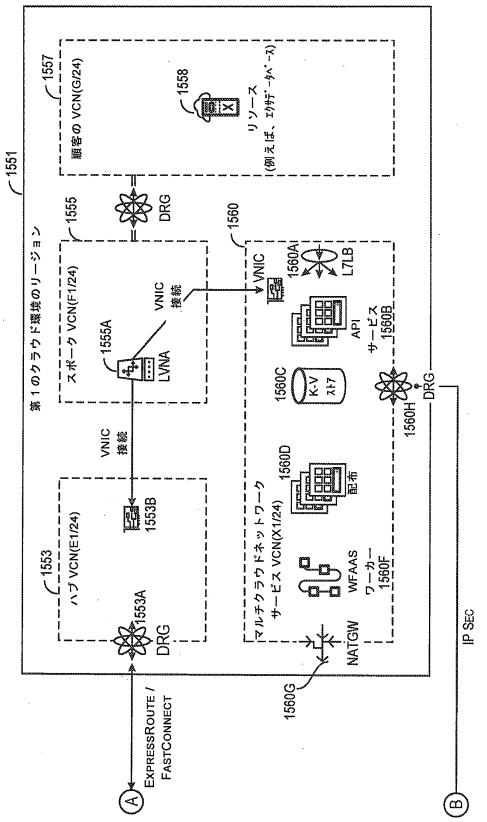

FIG. 15 (CONT.)

【図１６Ａ】

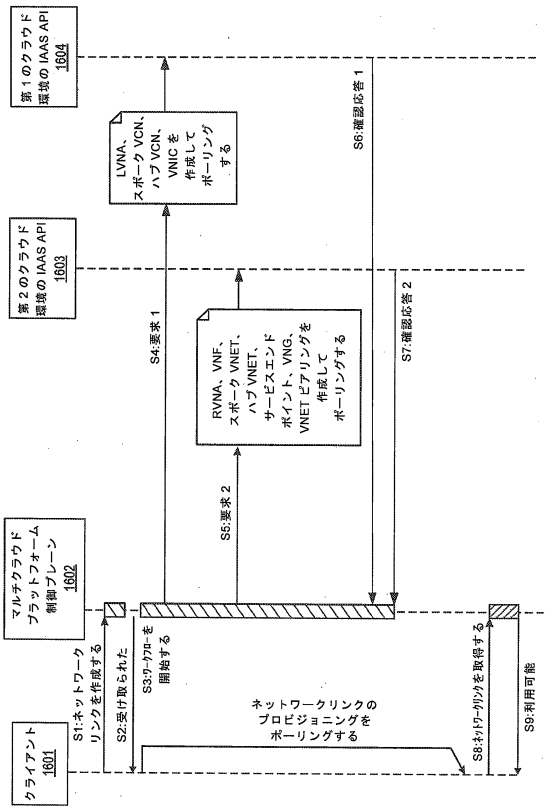

FIG. 16A

【図１６Ｂ】

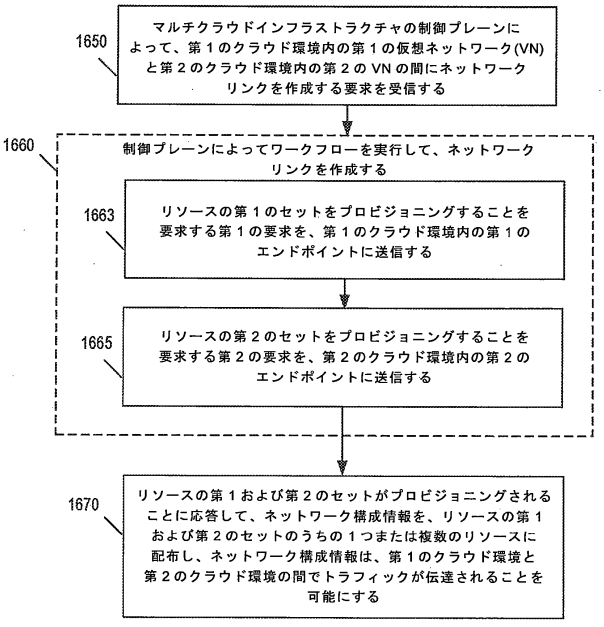

FIG. 16B

【図１７Ａ】

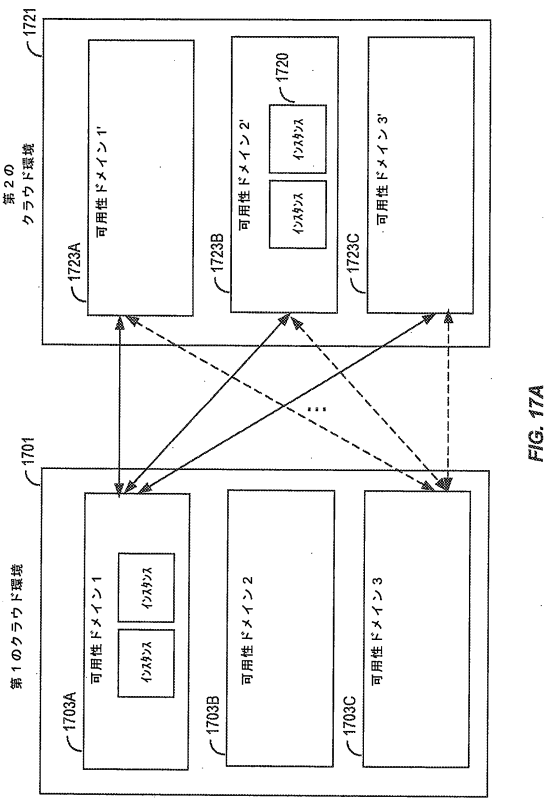

FIG. 17A

【図１７Ｂ】

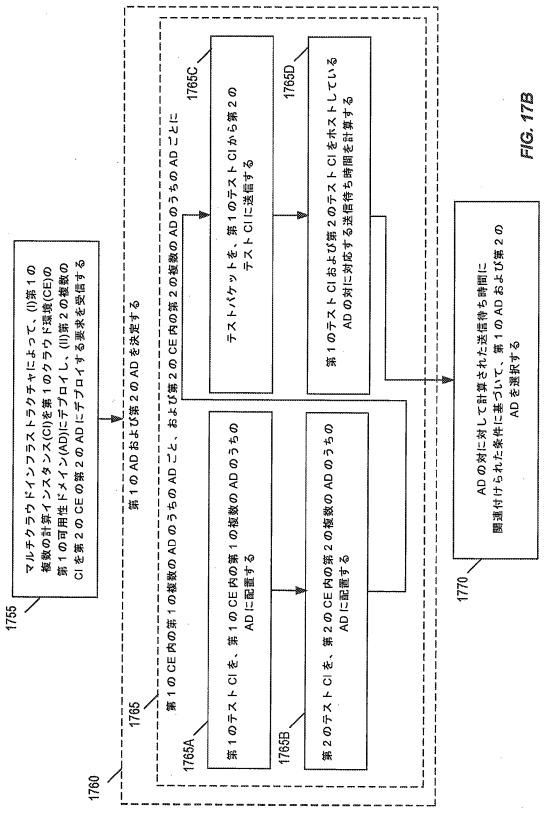

FIG. 17B

【図１８】

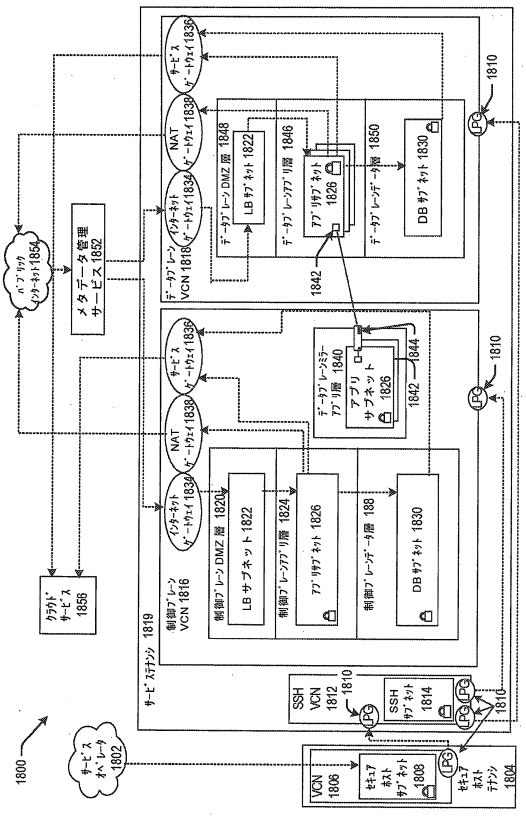

FIG. 18

【図１９】

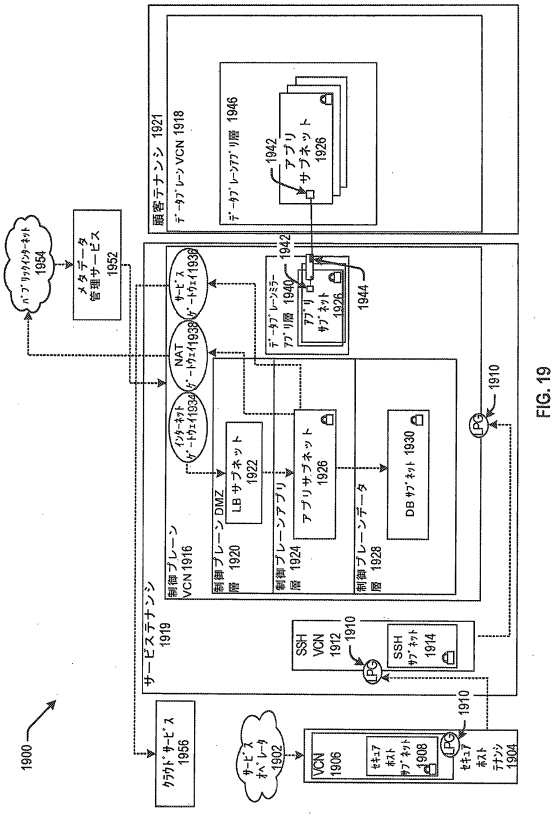

FIG. 19

【図２０】

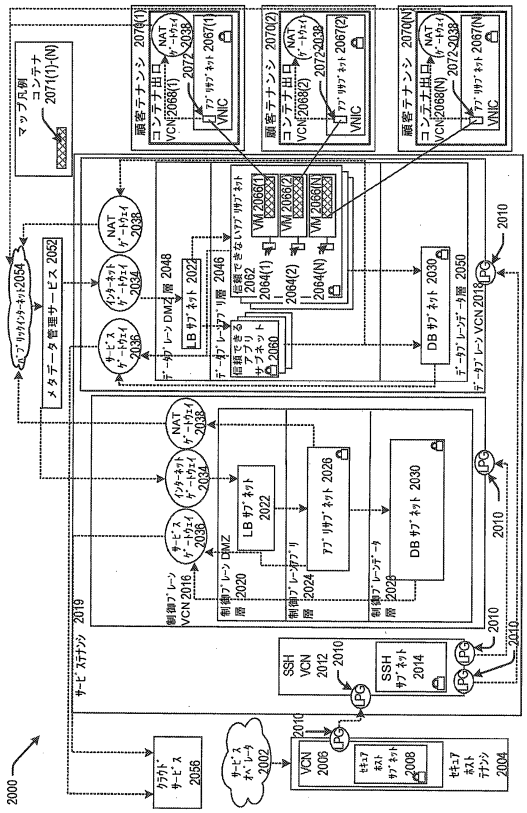

FIG. 20

【図２１】

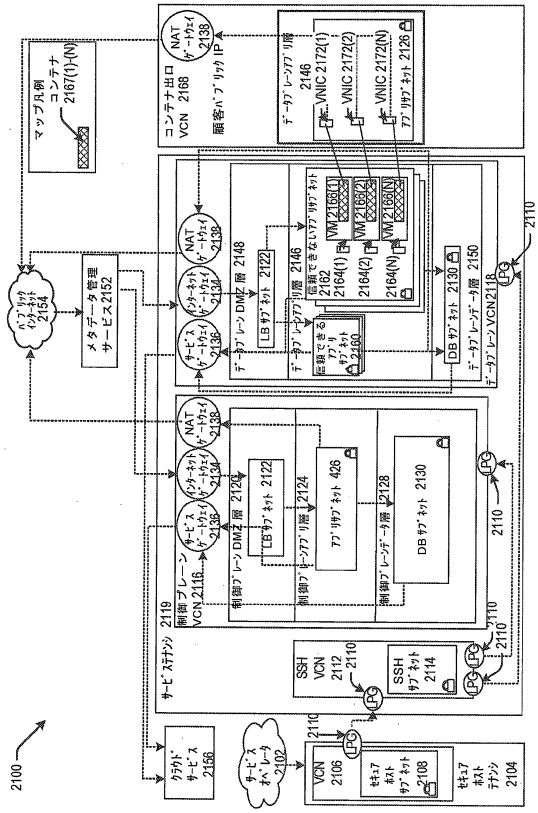

FIG. 21

【図２２】

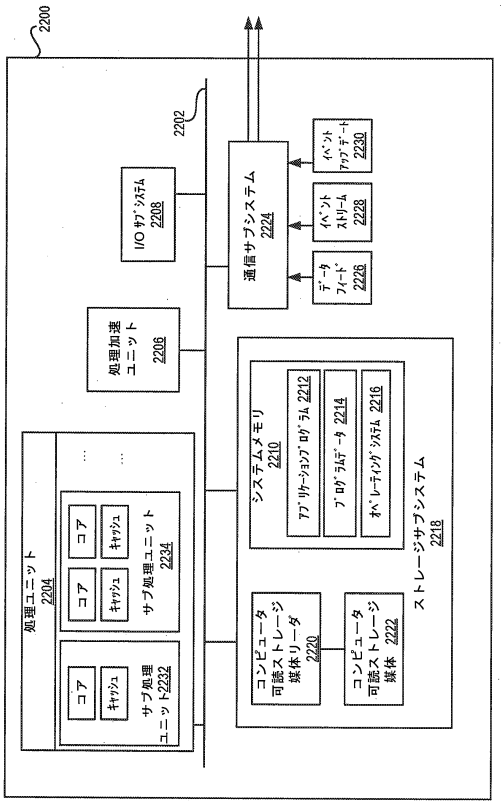

FIG. 22

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2023/061713

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F9/50 H04L12/46
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Arif Jamal: "How to setup the interconnect between Oracle Cloud Infrastructure and Microsoft Azure", , 20 June 2019 (2019-06-20), pages 1-22, XP093036741, Retrieved from the Internet: URL:https://medium.com/@j.jamalarif/how-to-setup-the-interconnect-between-oracle-cloud-infrastructure-and-microsoft-azure-da359233e5e9 [retrieved on 2023-03-31] the whole document -----	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 April 2023	20/04/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Touloupis, Emmanuel

Form PCT/ISA/210 (second sheet) (April 2005)

フロントページの続き

(32)優先日　令和4年3月18日(2022.3.18)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/333,965
(32)優先日　令和4年4月22日(2022.4.22)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/336,811
(32)優先日　令和4年4月29日(2022.4.29)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/339,297
(32)優先日　令和4年5月6日(2022.5.6)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/346,004
(32)優先日　令和4年5月26日(2022.5.26)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/389,145
(32)優先日　令和4年7月14日(2022.7.14)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/389,305
(32)優先日　令和4年7月14日(2022.7.14)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　63/380,326
(32)優先日　令和4年10月20日(2022.10.20)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,CV,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,ME,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＷＩＮＤＯＷＳ　ＰＨＯＮＥ
２．ＰＡＬＭ　ＯＳ
３．ｉＯＳ

(72)発明者　チャッカ，ジワラ・ディネシュ・グプタ
アメリカ合衆国、９４０６５　カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション内
(72)発明者　ブラール，ジャグウィンダー・シン

アメリカ合衆国、９４０６５ カリフォルニア州、レッドウッド・シティー、オラクル・パークウェイ、５００、オラクル・インターナショナル・コーポレイション内